TELECOMMUNICATIONS

IPL-AD2

ADSL router & RAS server & Firewall

User manual

Document reference : 9015509-03

The IPL-AD2 router is manufactured by

ETIC TELECOMMUNICATIONS

13 Chemin du vieux chêne
38240 MEYLAN
FRANCE

:

TEL : + 33 4-76-04-20-00
FAX : + 33 4-76-04-20-01
E-mail : hotline@etictelecom.com
web : www.etictelecom.com

OVERVIEW

INSTALLATION

../..

SETUP

../..

… SETUP

../..

… SETUP

../..

DIAGNOSTIC & MAINTENANCE

1 Products identification

IPL-AD2	1400	1220	1230
ADSL 2+ and RE-ADSL IP router	•	•	•
Firewall SPI	•	•	•
Remote access server - 25 users	•	•	•
25 VPN IPSEC & SSL	•	•	•
Serial gateway (Raw TCP and UDP, Telnet, Modbus, Unitelway)	-	•	•
RJ45 10 / 100 BT	4	2	2
RS232	-	1	2
RS485	-	1	-
IP router	•	•	•
NAT	•	•	•
Port forwarding	•	•	•
SNMP	•	•	•
DNS	•	•	•
DHCP client or server on the LAN interface	•	•	•
Digital input for alarm emails	1	1	1
HTML setup	•	•	•
IO Viewer : optional dynamic data html server	•	•	•

IPL-AD2-	1400B	1220B	1230B	1201B
Same functions plus :				
3G backup with an external USB modem				•
VRRP redundancy	•	•	•	•
IP addresses substitution	•	•	•	•
M2Me_Connect	•	•	•	•

• means the function is provided
- means the function is not provided

2 Product presentation

2.1 Overview

The IPL-AD2 ADSL router is a security product.

It is designed to interconnect safely automated devices over the Internet.

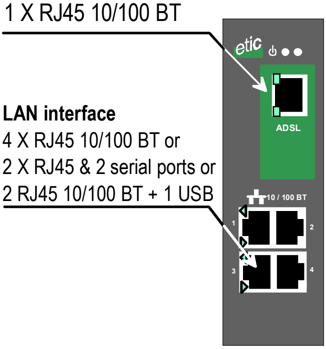
The IPL-AD2 is at the same time

- **an IP router** to route IP packets and set VPNs with other routers through the Internet.

- **a remote access server (RAS)** to provide a secure access to the LAN for remote users;

- **a stateful inspection firewall** to filter the IP traffic.

The IPL-AD2 comes with two interfaces :



WAN interface
1 X RJ45 10/100 BT

LAN interface
4 X RJ45 10/100 BT or
2 X RJ45 & 2 serial ports or
2 RJ45 10/100 BT + 1 USB

The ADSL interface :
That ADSL 2+ and Reach Extended ADSL interface can be connected to a public or private ADSL line.

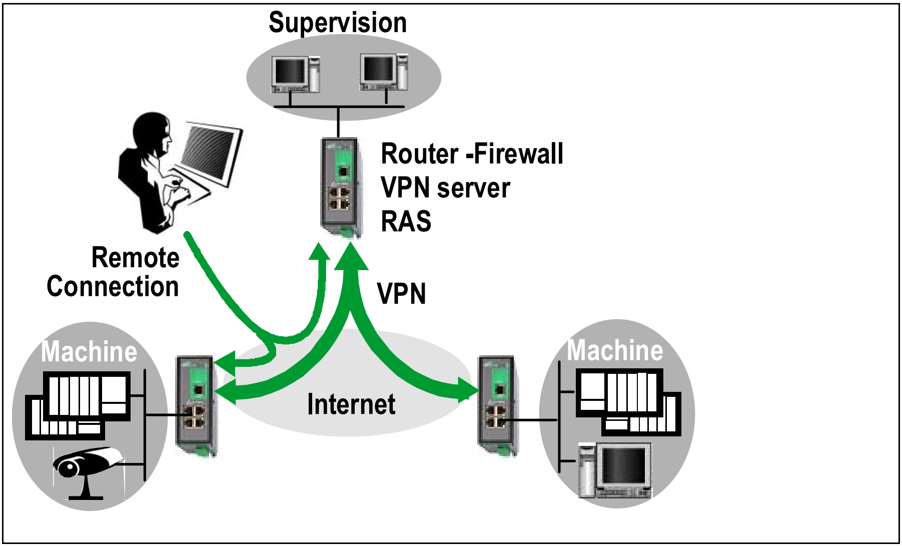
VPNs can be set on that interface.

Further in the text, this ADSL interface is called the WAN interface.

The LAN interface :
It is made to connect industrial devices.
Depending on the model, it includes
4 ethernet ports,
or 2 Ethernet and 2 serial ports,
or 2 Ethernet and 1 USB port.

2.2 Application

That features in the same product make the IPL-AD2 a top level solution for remote control systems through the Internet and remote maintenance.



2.3 Main functionalities

The IPL-AD2 router provides the functions hereafter :

IP router

The IPL-AD2 router provides powerful, flexible and comprehensive solutions to route IP packets from one network to other networks.

The solutions include remote nodes description, static routes, RIP protocol and destination network address translation (DNAT).

Safe VPN links

The IPL-AD2 router is able to establish safe VPN tunnels.

Once a VPN is established between two IPL-AD2 routers , each IP device connected to the first LAN can exchange IP packets with any device connected to the other LAN as if they were linked with a private line.

The IPL-AD2 router is able to establish up to 25 IPSec or TLS – SSL VPNs.

Authentication can be carried out with a pre-shared key or with certificates.

SPI Firewall

The IPL-AD2 incorporates a firewall. It is able to check source and destination IP addresses and ports number from the Internet and from the LAN.
The firewall also controls the status of the sessions (TCP, UDP, ICMP) to avoid sophisticated spoofing attacks.

Remote access server function

The IPL-AD2 provides to authorized users a remote access service to the devices connected either to the LAN or to a serial RS232-RS485 interface, as if his PC was directly connected to the LAN or to the RS232.

VRRP redundancy

Thanks to VRRP, a group of two or more routers can service the hosts of one subnet instead of only one usually; only one router of that group actually routes packets; if it fails another one of the group takes its place.

GSM-3G backup

The IPLAD2-1201B router provides a GSM-3G backup function when the ADSL connection fails.
A 3G USB modem must be connected to the USB interface of the IPL-AD2 router.
When the ADSL connection to the Internet provider fails, the IPL-AD2 router routes the data through the 3G network.

Serial gateway

The product includes an up-to-date RS to IP gateway, enabling to connect asynchronous devices directly and safely to the Internet.

Emails – sms

An email (or SMS) can be sent each time the digital input is opened or closed.

DNS server

DNS makes it possible to assign Internet names to devices or organizations independently of their public IP address.
The IPL-AD2 router behaves like a DNS server for the devices connected to the LAN.

DynDNS client (WAN interface)

The IPL-AD2 router is compatible with the Dyn DNS service

DHCP server (LAN interface)

DHCP is a standard Internet protocol that enables a DHCP server to dynamically distribute IP addresses and configuration information to the network DHCP clients.
Over the LAN interface, the IPL-AD2 can be a DHCP server.

SNMP

The IPL-AD2 router is an SNMP agent.

Html and DIP switches configuration

The IPL-AD2 is configured with a web server .
Two DIP switches allow to set the method the products receives its IP address over the LAN interface : From a DHCP client or server, factory IP address or stored IP address.

EticFinder software

The ETICFinder software is delivered with the product.
It detects the ETIC products connected to an Ethernet interface and displays the MAC address and the iP address of each product.

M2Me ™ VPN client software

M2Me is a TLS client software (to order separately) edited by ETIC Telecommunications.
It is able to register up to 100 VPN connections the user can set on a click.

3 Technical data

General characteristics	
Dimensions	137 x 48 x 116 mm (h, l, p)
Electrical safety	EN 60950- UL 1950
CEM	ESD : EN61000-4-2 : Discharge 6 KV RF field : EN61000-4-3 : 10V/m < 2 GHz Fast transient : EN61000-4-4 Surge voltage : EN61000-4-5 : 4KV line / earth
RoHS	2002/95/CE (RoHS)
Supply voltage	IPL-AD2-1400 & IPL-AD2-1230 : 10 to 60 VDC - 250 mA at 24 VDC IPL-AD2-1220 : 10 to 30 VDC - 250 mA at 24 VDC
Operating T°	-20°C / + 60°C Humidity 5 - 95 %

ADSL2 + transmission	
Cable	1 telephone grade twisted pair
ADSL	ITU G992.5 (ADSL 2 plus and Reach Extended ADSL)
Provider connection	PPPoEthernet or PPPoATM EoA : Ethernet over ATM RFC2684 Bridged IPoA : Routed IP over ATM, RFC2684 Routed
Data rate	Download 24 Mbit/s (From Internet) Upload 1 Mbit/s (To Internet)

Ethernet / IP router	
Ethernet	10/100 BT – 2 or 4 switched ports
IP router	Remote connections- static routes - RIP V2
Ip address translation	Source IP @ translation (NAT) Destination IP @ translation (DNAT) Port translation (Port forwarding)
DNS	Domain name
IP address assignment	Fixed IP @ or DHCP client or DHCP server

Security	
VPN	Client or server IPSEC or TLS/SSL Encryption 3DES Certificate X509 or preshared key
Firewall	Stateful packet inspection (50 rules)
Logs	Date and time stamped logs

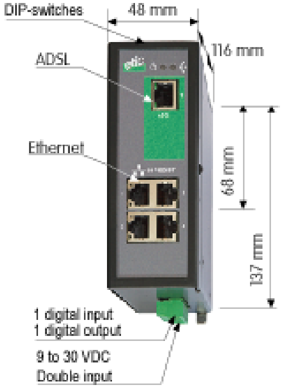
Remote access server (RAS)	
User list	25 users
Connection	VPN PPTP / L2TP-IPSec / TLS Open VPN Login & password Certificate X509
M2Me	VPN Compliant with the M2Me_Secure VPN client Compliant with the M2Me_Connect mediation service
Alarms	3 inputs : emails

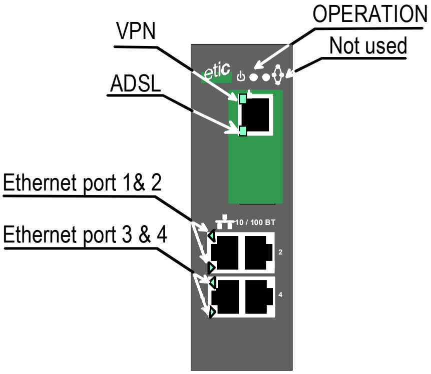
Serial interface	
RS232	1200 - 115200 kb/s parity N / E / O
Serial to IP gateways	Modbus master and slave Raw TCP client and server Telnet RAW UDP “multicast” unitelway

1 Product description

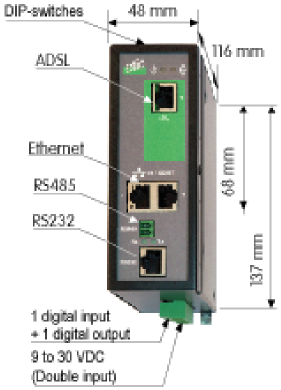
1.1 Overview

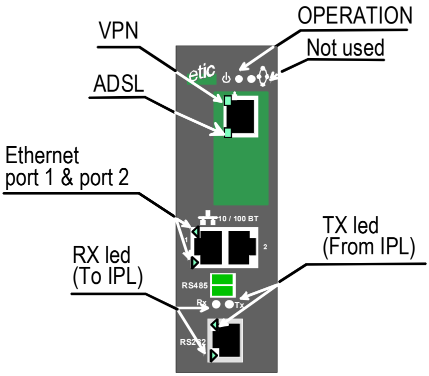
IPL-AD2-1400 and IPL-AD2-1400B



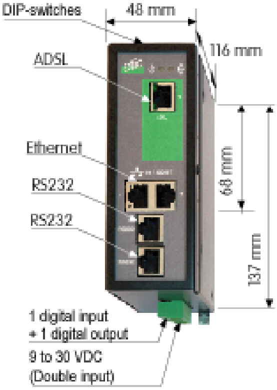


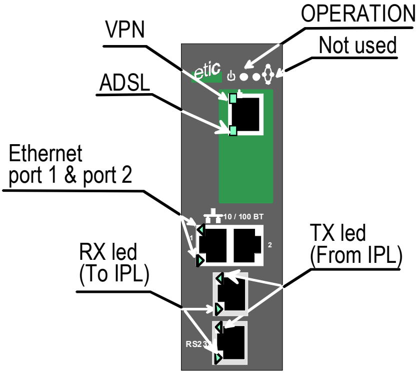
IPL-AD2-1220 and IPL-AD2-1220B



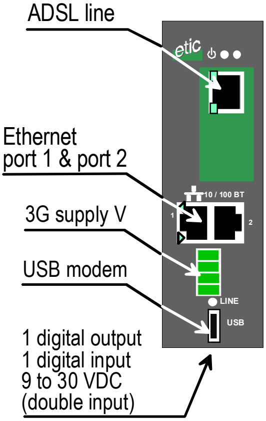


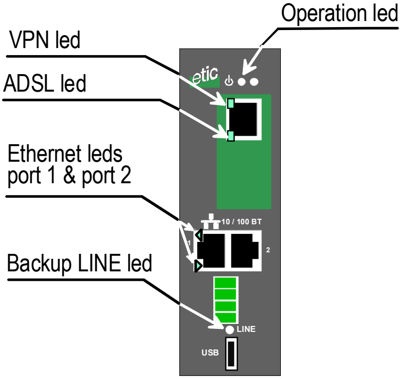
IPL-AD2-1230 and IPL-AD2-1230B





IPL-AD2-1201B





1.2 Leds

Interface	Led	Function
ADSL	VPN	One VPN at least has been established
ADSL	LINE	Blinking : ADSL connection in progress Lit : ADSL connection set
Ethernet	Ethernet 1 to Ethernet 4	Blinking quickly : Data activity Lit : Interface connected, no activity
RS232	Rx	Bytes received from the RS232 (to the IPL)
	Tx	Bytes transmitted to the RS232 (from the IPL)
RS485	Rx	Bytes received from the RS485 (to the IPL)
	Tx	Bytes transmitted to the RS485 (from the IPL)
USB	LINE	Lit : The 3G backup link is in operation Off : The 3G backup link is not in operation
	⏻	Green : Operation Red : Alarm

1.3 Connectors

8 pins screw block Supply voltage and input / output		
Pin Nr	**Signal**	**Function**
1	Power 1 +	10 to 60 VdC (IPL-AD2-1400 & IPL-AD2-1230) 10 to 30 VDC (IPL-AD2-1220)
2	Power 1 -	0 V
3		Reserved
4		Reserved
5	3V3	+ 3.3 VDC voltage provided by the product
6	In	Input
7	F +	Output + (max 50Vdc - 0,6A)
8	F -	Output -

ADSL RJ45 connector

Pin Nr	Signal	Function
1	N.C.	-
2	N.C.	-
3	N.C.	-
4	TIP	ADSL line
5	RING	ADSL line
6	N.C.	-
7	N.C.	-
8	N.C.	-

Ethernet RJ45 connector

Pin Nr	Signal	Function
1	Tx +	TX polarity +
2	Tx -	TX polarity -
3	Rx +	Reception polarity +
4	N.C	-
5	N.C	-
6	Rx -	Reception polarity -
7	N.C.	-
8	N.C.	-

RS485 2 pins screw block

Pin Nr	Signal	Function
1	A	RS485 polarity A
2	B	RS485 polarity B

RS232 RJ45 connector
(To connect to a DCE to the RS232 port)

Pin Nr	Circuit		Function
1	DTR - 108	OUT	Data terminal ready
2	TD - 103	OUT	Data Emission
3	RD - 104	IN	Data Reception
4	DSR - 107	IN	Data set ready
5	SG - 102	-	Ground
6	Not used	OUT	-
7	CTS - 106	IN	Clear to send
8	RTS - 105	OUT	Request to send

RS232 : RJ45 connector (To connect a DTE to the RS232 port)			
Pin	**Circuit**	**Direction**	**Function**
1	CD - 109	OUT	Carrier detect
2	RD - 104	OUT	Data Reception
3	TD - 103	IN	Data Emission
4	DTR - 108	IN	Data terminal ready
5	SG - 102	-	Ground
6	DSR - 107	OUT	Data set ready
7	RTS - 105	IN	Request to send
8	CTS - 106	OUT	Clear to send

4 pins screw block 3G modem power supply control (IPL-AD2-1201B)		
Pin	**Signal**	**Function**
1	V+OUT *	3G modem power supply output
2	V+IN	Supply voltage input
3	TO-IN	Active high signal used to switch on the modem TO_IN H > 5 VDC TO_IN L< 0,5 VDC Power ON t > 1 s
4	HR_IN	Active high signal used to switch off the modem HR_IN H > 5 VDC HR_IN L< 0,5 VDC Power OFF 1 s< t < 2s

1.4 DIP-switches & push-button

DIP switches		
SW 1	**SW 2**	**Management**
OFF	OFF	The current IP@ of the product is the stored IP @
ON	OFF	**The active IP@ of the product is the factory IP@ : 192.168.0.128** **No login and password are required to access to the html server**
OFF	ON	The active IP@ is provided by the BOOTP or DHCP server.
ON	ON	Reserved

Push-button : It enables to restore the factory profile.
To restore the factory profile, switch the power on while pressing the push-button until the RUN light turns green.

Attention : Once the factory profile has been restored, the stored configuration is lost.

2 Ventilation

To avoid overheating when the ambient temperature is high, leave a 1 cm (0.5 inch) space on each side of the product.

3 Supply voltage

IPL-AD2-1400 and IPL-AD2-1230 : The supply voltage must be strictly lower than 60 VDC and higher than 10 VDC. The consumption is 250 mA at 24 VDC.

IPL-AD2-1220 : The supply voltage must be strictly lower than 30 VDC and higher than 10 VDC. The consumption is 250 mA at 24 VDC.

4 Ethernet ports

The IPL-AD2 features two or four auto-sensing 10/100 Mbps MDI/MDI-X LAN ports.

5 RS232 interface

The RS232 data rate can be tuned from 1200 to 115200 b/s with parity (even / odd) or no parity.

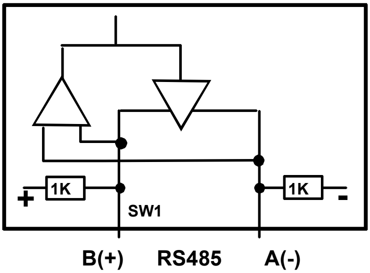
The data terminal must be less than 10 meters far from the modem.

Cables can be provided to connect the product to DTE and DCE as follows :

RS232 cables (L=1m)		
Code	**User connector**	**Cable function**
CAB592	SubD 9 male	To connect a DCE to the IPL-AD2
CAB593	SubD 9 female	To connect a DTE to the IPL-AD2
CAB609	wires	To connect a device providing a specific connector

6 RS485 interface

The RS485 serial interface is provided on the front panel 2 pins screw-block.

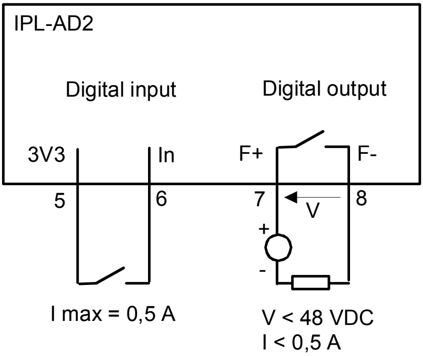


Polarisation resistors
1 Kohm bus polarisation resistors are included inside the product.

RS485 line adaptation
For a several meters long connection over the RS485 local interface, it is not necessary to adapt the RS485 line. For a longer distance, connect a 120 Ohm resistor at each end of the line.

7 Input & output connection

Alarm output
1 relay output is provided to indicate an alarm.
The alarm condition can be selected using the html server.



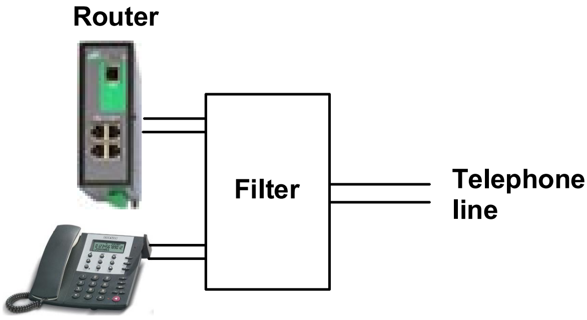
The electrical characteristics of the output are :
Opto-isolated output
Maximum voltage : 50 VDC
Maximum current : 500 mA

Inputs
The product features two digital inputs ; they are not isolated.
if one input is opened, an SNMP trap will be sent to the SNMP server is that function has been enabled.

8 Line connection

The IPL-AD2 is designed to be connected to an analog line.

If an analog telephone set has to be connected to the line ; a filter has to be added to separate the ADSL signal from the voice signal.



9 Internet subscription

IP address :
The IP address is generally assigned by the provider ; it can also be entered.

If it is assigned by the provider and if it is a temporary IP address, the product has to be a VPN client over the Internet ; it will connect to a VPN server device to which a fixed IP address will have to be assigned.

If a fixed IP address cannot be assigned to the VPN server device, one can use the DYNDNS service which enables to use a domain name instead of an IP address (see Configuration chapter).

Other technical parameters :
See Configuration chapter. paragraph 5.4.

1 Setup steps

To configure the router, we advise to proceed as follows :

- Connecting a PC to the router
- Setting up the LAN and WAN interfaces
- Setting up VPNs
- Setting up routing and IP address translation functions
- Setting up remote connections and the M2Me_Connect service
- Setting up the remote users list
- Setting up the firewall

The IPL-AD2 router is configured with a PC and an HTML browser.
2 DIP switches enable you to set the IP address : Factory address, stored address, BootP or DHCP client or server.

For the first configuration, we advise to connect the PC directly to the router Ethernet interface.

Modifications can be carried out through the LAN or remotely.

2 Configuring the router

2.1 Overview

The IPL-AD2 router is configured with a PC and an HTML browser.

Administration server address :
The administration html server is located at the LAN IP address of the router (The default address is192.168.0.128).

First setup :
For the first configuration, we advise to connect the PC directly to the LAN interface of the IPL-AD2 router.

Setup modifications :
Modifications can be carried out from the LAN interface, or from the Internet if a firewall rule authorises to reach the administration server (not advised), or from the Internet or using a remote user connection or a VPN.

Restoring the factory IP address :
The factory IP address of the router on the LAN interface can be restored by setting the DIP switches SW01 ON and SW02 OFF.
In that position o the DIP switches, the stored configuration is not deleted.
Setting the DIP switches in that position gives also a free access to the administration server from the LAN interface.
During operations, the DIP switches must not be left in that position.

Network IP address :
Later in the text, we often speak of "network address".
We mean the lowest value of the addresses of the network.
For instance, if the netmask of a network is 255.255.255.0, the network address of that network is X.Y.Z.0.

Copy and paste :
Parameters must be entered with the keyboard; they cannot be pasted.
However, it can be useful to paste a string when it is long to avoid errors.
In that case, paste the string, delete the last character of the pasted string, and enter it again with the keyboard.

Saving and restoring the parameters file (see the maintenance chapter)
A parameters file can only be downloaded to a product having the same firmware version.
It is why, we advise to assign a name to a parameter file including the product name and the software version like for instance "myrouterfile_iplad21220_V241.bin".

2.2 First configuration

Step 1 : Check the DIP switches

Coming from factory, the DIP switches SW1 and SW2 are set OFF to select the stored IP address.
Coming from factory, the stored IP address is the factory IP address 192.168.0.128.

Step 2 : Create or modify the PC IP connection.

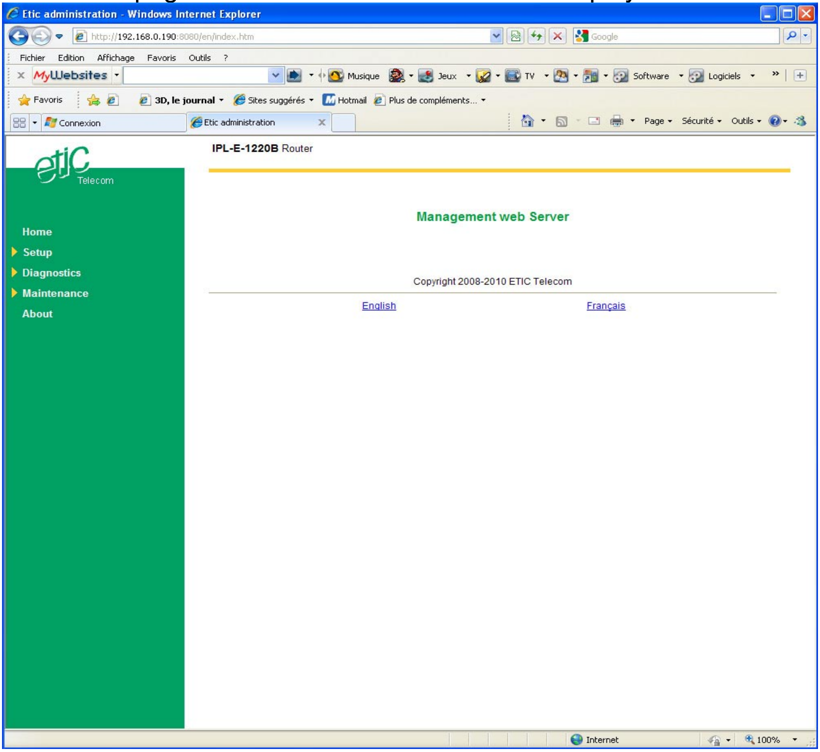
Assign to the PC an IP @ in accordance with the IPL-AD2 IP address.
For the first configuration, assign or instance 192.168.0.127 to the PC.

Step 3 : Connect the PC directly to the LAN interface of the IPL-AD2 router using any Ethernet cable (straight or cross wired).

Step 4 : Launch the navigator

Enter the LAN IP @ of the router 192.168.0.128.

The Home page of the administration server is displayed



Etic administration - Windows Internet Explorer

http://192.168.0.190:8080/en/index.htm

IPL-E-1220B Router

Management web Server

Copyright 2008-2010 ETIC Telecom

Remark :
If the home page cannot be displayed, refer below.

2.3 Modifying the configuration parameters through the LAN

- **If the IP @ of the IPL-AD2 on the LAN interface is assigned by a DHCP server**

Step 1 : Ensure the DIP switch SW1 is OFF and SW2 ON to select DHCP client operation.

Step 2 : Launch ETIC FINDER to detect the IPL-AD2 address over the LAN interface.

Click the product once detected.

The Home page of the administration server is displayed.

Remark :
If the home page cannot be displayed, refer below.

- **If the IP @ of the IPL-AD2 on the LAN interface is fixed**

Step 1 : Ensure the DIP switch SW1 and SW2 are OFF to select the stored IP @.

Step 2 : Launch the html browser and enter the IP address assigned to the router.

Or, launch the ETICFINDER utility to detect the IPL-AD2 address.

Remark :
If the home page cannot be displayed, refer below.

2.4 Modifying the configuration from the Internet

Coming from factory, the firewall rejects all the packets coming from the Internet to the LAN.

To carry out modifications from the internet, it is possible to set a remote user PPTP or TLS connection.

The modifications can be also carried out from a remote LAN through a VPN.

3 Rebooting the router after parameters changes

- After the parameters any page have been completed, click the « Save » button at the bottom of the page.

- After some parameters changes, the IPL-AD2 must restart. When the configuration has been completely carried out, click the « Reboot » red button in the green bar, when displayed.

- Once the product has restarted, check the « Reboot » button has disappeared from the green bar.

To save the configuration file to a hard disk :

- Select the “maintenance” menu and then the “Save / restore” menu.

- Click the “Save current configuration to disk” button.

4 Recovering the factory LAN IP address

When launching the html browser, the homepage of the html server may not be displayed; the cause may be the IP address you entered was wrong.

if the IP address you enter is wrong, you can recover the factory IP address by setting SW01 ON and SW2 OFF.
The factory IP address 192.168.0.128 will be restored as long as the SW01 and SW02 micro switch will be left in that position.

Remark :
The SW01 and SW02 must not be left in that position during operations.

5 Recovering the factory configuration

If firewall rules have been created finally preventing from reaching any IP address on the LAN interface including the router itself, it may be necessary to restore the factory configuration of the router.

To restore the IPL-AD2 factory configuration,

- Switch OFF the power supply of IPL-AD2 router.

- Press the push button on the top part of the IPL-AD2 router and switch ON the power supply.

- Keep the push button pressed until the operation led turns red.

Remark : The stored configuration will be lost; the factory IP address 192.168.0.128 will be restored.

6 Restricting access to the administration server

The access to the administration server can be protected by a login and password.

To protect access to the administration server,

- Select the “Setup” menu, the “Security” menu and then the “Administration menu”.

Remark : For more simplicity, we advise to chose the login and the password of one of the remote users stored in the user list.

7 Recovering a free access to the administration server

If the Login & or password entered to reach the administration server have been rejected, it is possible to recover a free access to the administration server from the LAN only, by setting SW01 ON and SW2 OFF.

Remark :
The factory IP address 192.168.0.128 will also automatically be restored as long as SW01 will remain ON and SW2 OFF.
During normal operations SW01 and SW02 must not be left in that position.

8 Factory configuration

Coming from factory, the router configuration is as follows :

LAN IP @	192.168.0.128
WAN IP @	None
Default user :	Login = admin ; Password = admin
Admin. server restriction :	None

Firewall :

Remote user filter	Authorises any remote user belonging to the user list to reach a LAN IP address using a PPTP or TLS or L2TP / IPSec connection
Main filter	IP packets coming from the Internet to the LAN are dropped. IP packets transported inside a VPN are forwarded

9 Assigning an IP address to the LAN interface

9.1 IP addresses

To set up the LAN interface IP parameters,

- Click the « **Configuration**» menu and then « **LAN interface**» and then "**IP protocol**".

LAN parameters :

IP address :
Enter the IP address assigned to the router over the Ethernet local network.

Netmask :
Enter the IP netmask assigned to the local network.

Remote access parameters :

Start of users IP address pool **and** **end of users IP addresses pool :**
That parameters define the pool of addresses which will be assigned automatically to remote user's PC when they will connect to the router.
Enter the start address and the end address.

Remark :
After the LAN IP address of the router has been modified, it is necessary to reboot the unit.

Moreover, If VPNs have been created, they must be launched again.
To launch the VPNs again after the LAN IP address has been modified,

- Select the « network» menu and then the « **VPN** » menu,
- Click the « Properties » button in front of the « type of VPN » field, and then on the "OK" button of the window entitled« VPN properties».
- Click the « Modify » button in front of the « VPN connection » field, and then on the "OK" button.

If the DHCP server is used, it must be also launched again.
To launch again the DHCP server after the LAN IP address has been modified,

- Select the « LAN interface» menu and the «DHCP server» menu,
- Unselect the « Enable the DHCP serve» checkbox, and then select it again.

9.2 DHCP server configuration

Over the LAN interface, the IPL-AD2 router can behave like a DHCP server.
If you select that option, we advise to assign a fixed IP address to the IPL-AD2 router itself over the LAN interface.

To configure the DHCP server function,

- select the « **Setup**» menu and then « **LAN interface**» and then « **DHCP server** ».
-

<u>“IP address pool start” & “IP addresses pool end” parameters</u> :
That parameters define the range of IP addresses which can be assigned by the IPL-AD2 to the DHCP client devices.

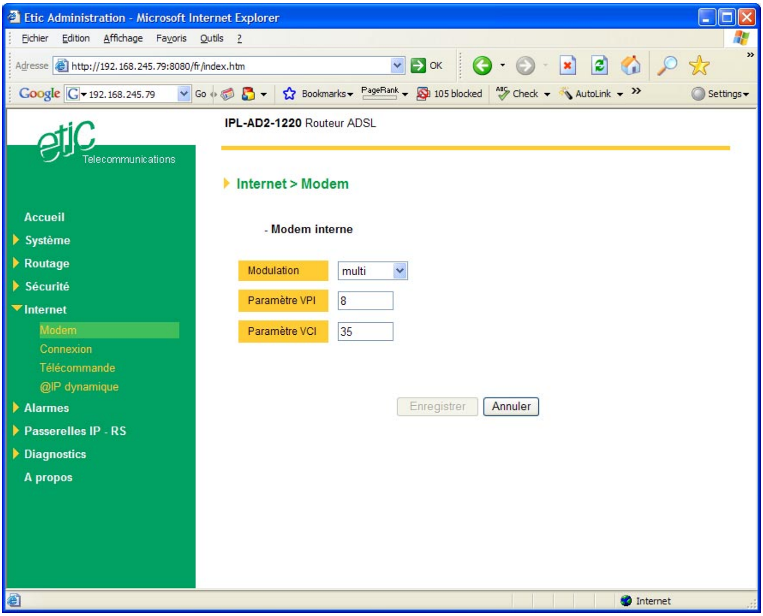
-

<u>“Primary DNS IP address”</u>   & “<u>secondary DNS IP address” parameters</u> :
Enter the IP addresses of the domain name servers.; the DHCP server will communicate that information to the DHCP client devices.

10 Internet connection

10.1 ADSL parameters

Select the “**Configuration** “ menu, the “**WAN interface**” menu and then the « **Modem** » menu.



Etic Administration - Microsoft Internet Explorer

IPL-AD2-1220 Routeur ADSL

Internet > Modem

- Modem interne

Modulation: multi

Paramètre VPI: 8

Paramètre VCI: 35

That menu allows to select the way the ADSL modem connects to the provider modem (DSLAM).

”Modulation” parameter :

The default value is multi; the modem will adapt to the modulation of the FAI modem.

Otherwise, ask your provider.

“VPI” parameter :

This parameter is used to set the « Virtual Path Identifier » for the APVC.

Range is 0 - 255.

“Virtual Path Identifier” & “Virtual Channel Identifier” parameters :
This parameter is used to set the Virtual Channel Identifier for the APVC. Range is 0 - 65535.

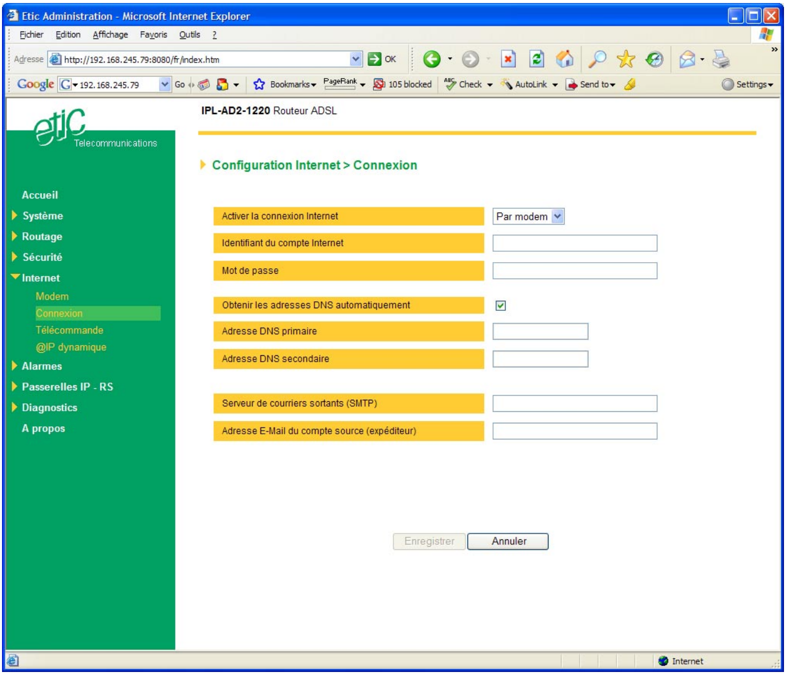
“Multiplexing” parameter :
LLC : Select LLC or VC

“Encapsulation” parameter :

Option	Description
PPPoA VC-Mux	RFC 2364 VC-multiplexed PPP over AAL5
PPPoA LLC	RFC 2364 LLC encapsulated PPP over AAL5
PPPoE VC-Mux	RFC 2516 VC-multiplexed PPP over Ethernet
PPPoE LLC	RFC 2516 LLC encapsulated PPP over Ethernet
Bridged Ethernet VC-Mux	RFC 2684 VC-multiplexed bridged Ethernet
Bridged Ethernet LLC	FC 2684 LLC encapsulated bridged Ethernet

10.2 Internet connection parameters

Select the « **Internet** » menu and then click« **Connection** ».


Etic Administration - Microsoft Internet Explorer
Fichier Edition Affichage Favoris Outils ?
Adresse http://192.168.245.79:8080/fr/index.htm
OK
Google 192.168.245.79 Go Bookmarks PageRank 105 blocked Check AutoLink Send to Settings
Telecommunications
Accueil
Système
Routage
Sécurité
Internet
Modem
Connexion
Télécommande
@IP dynamique
Alarmes
Passerelles IP - RS
Diagnostics
A propos
Internet

IPL-AD2-1220 Routeur ADSL

Configuration Internet > Connexion

Activer la connexion Internet	Par modem
Identifiant du compte Internet	
Mot de passe	
Obtenir les adresses DNS automatiquement	☑
Adresse DNS primaire	
Adresse DNS secondaire	
Serveur de courriers sortants (SMTP)	
Adresse E-Mail du compte source (expéditeur)	

Enregistrer Annuler

The information entered in this page have to be provided by the Internet provider.

“Internet account” parameters : Refer to your Internet contract

“Internet account password” parameters : Refer to your Internet contract

“Service name” parameter : Refer to your Internet contract

“Obtain an IP address automatically” parameter :
Set that option if the provider is supposed to assign an IP address to the router through the line each time it connects to the Internet.

“IP address” & “netmask” parameter :
Enter the fixed IP address and netmask assigned to the router if it not assigned through the line.

“Obtain DNS IP addresses automatically” parameter : Select that option if the Domain name servers IP addresses are supposed to be provided automatically through the Internet.

“Primary DNS IP address” & “secondary DNS IP address” parameters :
Enter the IP addresses of the domain name servers.

”SMTP server” parameter :
It the address of the SMTP server for outgoing mails (ex : smtp.nerim.net)

“Source account e-mail address” parameter :
Enter the email address attached to the account.

10.3 Internet connection control

- Select the « Internet » menu and then click« remote control ».

Connect to Internet at product power-on :
If that option is selected, the router will connect to the Internet as soon it will be powered on.

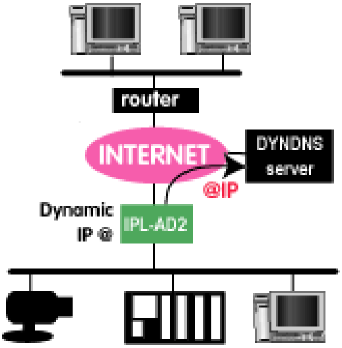
Connect to Internet on a rising edge of the digital input 1 :
If that option is selected, the router will connect to the Internet each time the digital input 1 will be set closed.

”Connect to Internet now” parameters :
The router will connect to the Internet when the button “Connect” will be clicked.

11 Releasing the dynamic IP @ with the DYNDNS service

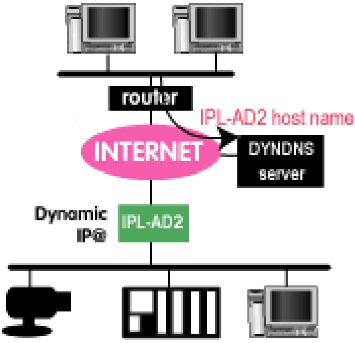
Dynamic DNS (DDNS) allows you to create a hostname that points to a dynamic IP or static IP address or URL.

If the IP address assigned to the router over the Internet is not fixed, the router will contact the DYNDNS service each time it will change and update the hostname table with the new address.



Each time a device wishes to connect to the IPL-AD2, it will use its host name and get its temporary IP address from the DYNDNS server or from another DNS server.

It will then connect to the IPL-AD2 as if its address had been fixed.



To configure that function,

- **go to www.dyndns.org and create an account.**
- **Select the « Wan interface » menu and then « DynDNS »**
  Enable the DYNDNS function.
  Enter the account login and password provided by DYNDNS
  Enter the hostname which has been registered (Ex : iplad2grenoble2.dyndns.org).

12 Creating VPN connections between routers

12.1 Principles

A VPN is a safe link set between two end-points over an IP network : Both routers authenticate, data are encrypted and each device of a LAN can exchange data with each device f the other one. (see appendix 1).

25 VPNs can be set on the WAN interface of the IPL-AD2 router.

Two types of VPN can be set : TLS VPN and IPSec VPN.

IPSec has the advantage to be a standard solution.

TLS is easier to employ because the transport layer is TCP or UDP; it is why, it can be easily used when the VPN must pass through several or even numerous company routers.

Once a type of VPN (TLS or IPSec) has been selected, all the VPN set between the IPL-AD2 router and another one must be the same.

Two steps are necessary to configure the IPL-AD2 to create VPN connections between routers :

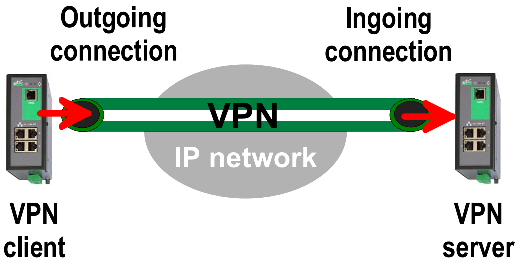
1st step : Select the type of VPN and setting the parameters
2 types of VPNs can be used to connect IPL-AD2 routers together or with other type of routers: IPSec or TLS/ SSL

Once a type of VPN has be selected, it applies to all the connections with remote routers.

2nd step : Create VPN connections

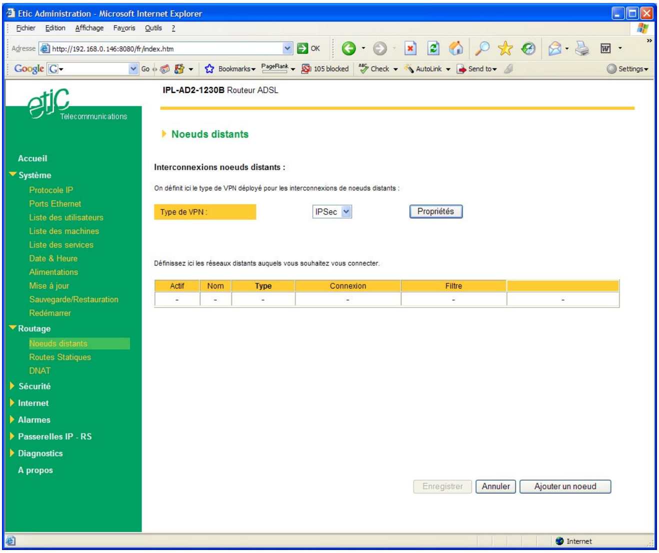
A connection can be an incoming connection or an outgoing connection.

If a connection is an incoming connection, the local router is named "VPN server" and the remote router is a "VPN client".



To create VPN connections between routers,

select the « **Setup**» menu and then « **Network**» and then “**V˙PN connections**”.



IPL-AD2-1230B Routeur ADSL

Noeuds distants

Interconnexions noeuds distants :

On définit ici le type de VPN déployé pour les interconnexions de noeuds distants :

Type de VPN : IPSec [Propriétés]

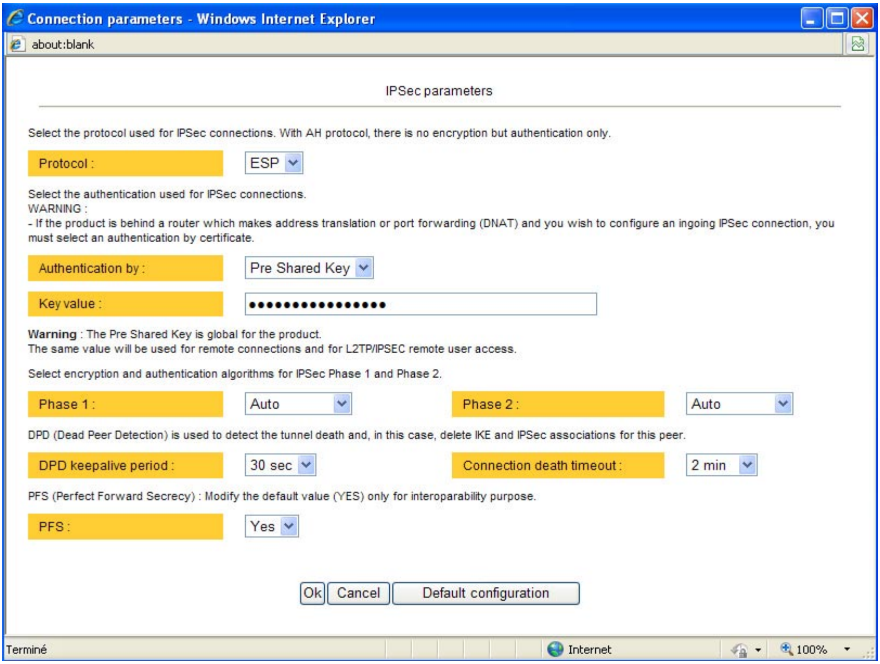
Définissez ici les réseaux distants auxquels vous souhaitez vous connecter.

Actif	Nom	Type	Connexion	Filtre	
-	-	-	-	-	-

12.2 IPSec VPN connections

12.2.1 Configuring the IPSec protocol

- Select the “**Setup**” menu, the “**network**” menu and then ‘**VPN connections**”.
- Select the “**Ipsec**” type of VPN,
- Click **“Properties**” .



IPSec parameters

Select the protocol used for IPSec connections. With AH protocol, there is no encryption but authentication only.

Protocol : ESP

Select the authentication used for IPSec connections.
WARNING :
- If the product is behind a router which makes address translation or port forwarding (DNAT) and you wish to configure an ingoing IPSec connection, you must select an authentication by certificate.

Authentication by : Pre Shared Key

Key value : ●●●●●●●●●●●●●●●●

Warning : The Pre Shared Key is global for the product.
The same value will be used for remote connections and for L2TP/IPSEC remote user access.

Select encryption and authentication algorithms for IPSec Phase 1 and Phase 2.

Phase 1 : Auto   Phase 2 : Auto

DPD (Dead Peer Detection) is used to detect the tunnel death and, in this case, delete IKE and IPSec associations for this peer.

DPD keepalive period : 30 sec   Connection death timeout : 2 min

PFS (Perfect Forward Secrecy) : Modify the default value (YES) only for interoparability purpose.

PFS : Yes

“Encryption Protocol” parameter :
Select ESP to encrypt the data flow; select AH, if no encryption is required or if NAT traversal is required.

“Authentication & encryption key” parameter :
Authentication an encryption can be carried-out with a pre-shared key or a certificate.

“Pre-shared key” value :
The pre-shared key value applies to all the connections.
The maximum length of the key is 40 characters.

The same preshared key value will be used for remote users L2TP / IPSec connections.

“Certificate” value
The IPL-AD2 router is delivered with a certificate stored into the product in our factory.
To add a certificate, refer to the “Security” menu.

“Encryption and hash algorithm phase 1” & “Encryption and hash algorithm phase 2” parameters :
That parameters allow to define the encryption and hash algorithms in use during the phase 1 of the exchanges between the end-points (VPN set-up) and during the phase 2 (data exchange).

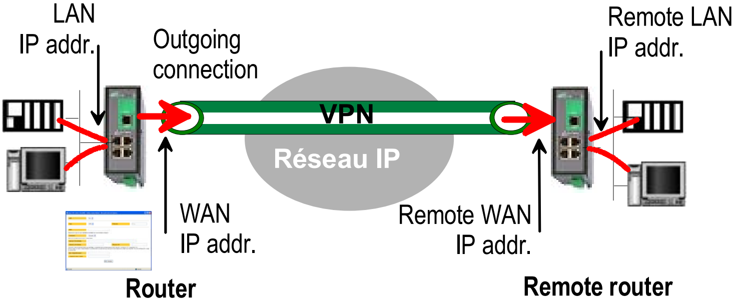
The default value is Auto; in that case both end-points will negotiate a common algorithm.

“DPD request period” parameters :
A DPD request (also called Keepalive message) is a message sent periodically by each end-point to the other one to make sure that the VPN must be left active.
This parameters sets the amount of time (in seconds) between two of these requests.

“Connection death time-out” parameters :
This parameter defines the maximum amount of time (in seconds) a VPN connection will stay established if no traffic or no DPD request message are received from the remote point.

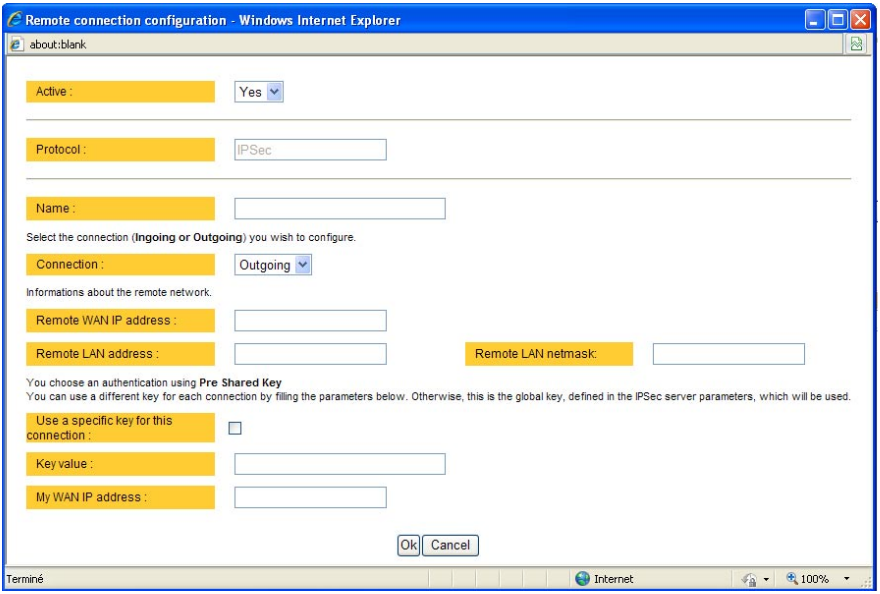
ATTENTION : Once the parameters of the IPSEC connection have been selected, click the OK button and then the Save button.

12.2.2 Configuring an outgoing IPSec connection



To set an outgoing VPN connection,

- Come back to the "**VPN connections**" screen,
- Click the "add a connection" button..



Active : Yes

Protocol : IPSec

Name :

Select the connection (**Ingoing or Outgoing**) you wish to configure.

Connection : Outgoing

Informations about the remote network.

Remote WAN IP address :

Remote LAN address : Remote LAN netmask:

You choose an authentication using **Pre Shared Key**
You can use a different key for each connection by filling the parameters below. Otherwise, this is the global key, defined in the IPSec server parameters, which will be used.

Use a specific key for this connection : □

Key value :

My WAN IP address :

Ok Cancel

Give a name to the connection and select **the "Outgoing" option.**

‘Remote WAN IP address’ parameter :
Enter the IP network address and netmask assigned to the remote router over the internet.

“Remote LAN address & Remote LAN netmask” parameters :
Enter the IP network address and netmask assigned to the remote LAN.

- **Preshared key**

If the preshared key used by the connection is the general PSK entered in the “VPN” menu, no additional parameter has to be entered.

If a particular PSK must be used, complete the configuration of the connection as explained below.

“Unique PSK for this node” parameters :
Select that option if a particular PSK key has to be used for this connection.

“PSK value” parameter :
Enter the value of the PSK.

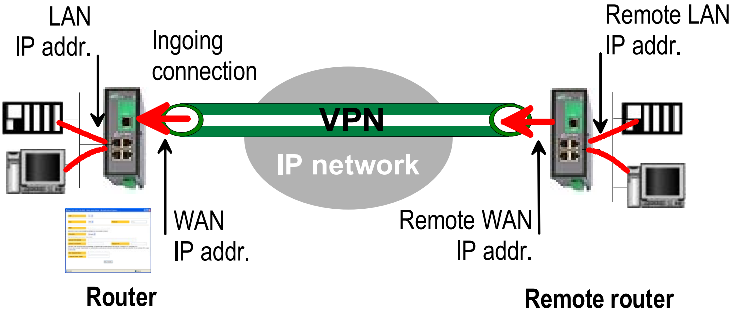
”My WAN address” parameter :
Enter the Internet IP address of the router

- **Certificate**

“My subjectAlt name” & “Remote subjectAlt name” parameters :
Paste the field "SubjectAltName" of the active certificate of the router you are configuring and the one the remote router.

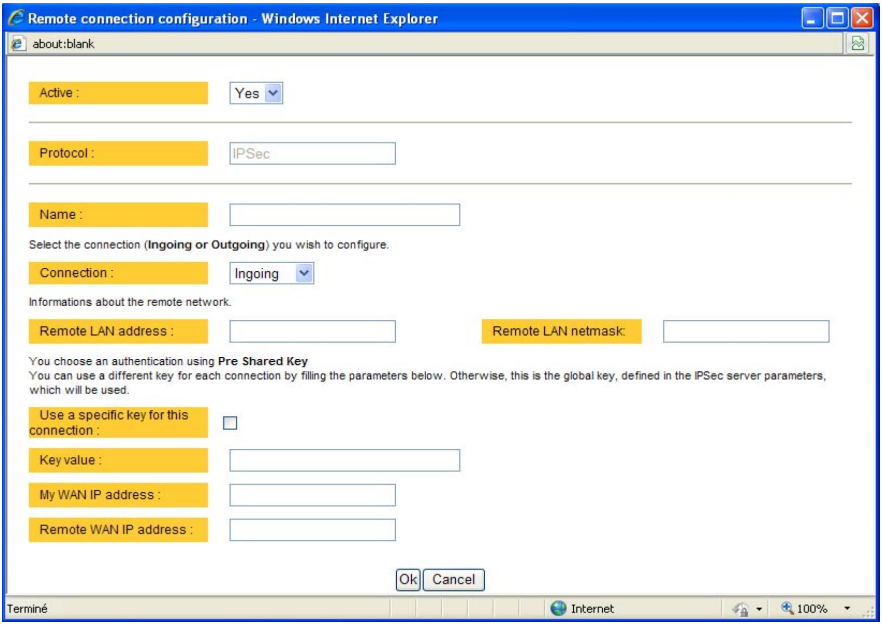
Attention : For ETIC certificates, this field is the Email field

12.2.3 Configuring an ingoing IPSec connection



To set an ingoing VPN connection,

- Come back to the “**VPN connections**” screen,
- Click the “add a connection” button.



Active :	Yes
Protocol :	IPSec
Name :	

Select the connection (**Ingoing or Outgoing**) you wish to configure.

Connection :	Ingoing

Informations about the remote network.

Remote LAN address :		Remote LAN netmask:	

You choose an authentication using **Pre Shared Key**
You can use a different key for each connection by filling the parameters below. Otherwise, this is the global key, defined in the IPSec server parameters, which will be used.

Use a specific key for this connection :	□
Key value :	
My WAN IP address :	
Remote WAN IP address :	

Give a name to the connection and select **the “ingoing” connection direction option**.

“Remote WAN IP address” parameter :
Enter the IP network address and netmask assigned to the remote router over the Internet (public IP address over Internet).

“Remote LAN address & Remote LAN netmask” parameter :
Enter the IP network address and netmask assigned to the remote LAN.

- **Preshared key**

If the key used by the connection is the general PSK entered in the VPN menu, no additional parameter has to be entered.

If a particular PSK must be used, carry out the configuration of the connection as explained below.

“Use a specific key for this connection” parameter :
If that option is not selected, the preshared key entered in the VPN configuration screen will be used by the router.
If that option is selected, enter the specific key.

“My WAN address” & “Remote WAN address” parameters :
Enter the WAN IP address of the router (public IP address over Internet) and the WAN IP address of the remote router (public IP address over Internet).

Attention : For ETIC certificates, this field is the Email field

- **Certificate**

“My subjectAlt name” & “Remote subjectAlt name” parameters   :
Paste the field "SubjectAltName" of the active certificate of the router you are configuring and the one the remote router.

Attention : For ETIC certificates, this field is the Email field.

12.3 Setting TLS VPN connections

12.3.1 Configuring the TLS-SSL protocol

- Select the “**Setup**” menu, the “**network**” menu and then the ‘VPN connections” menu.

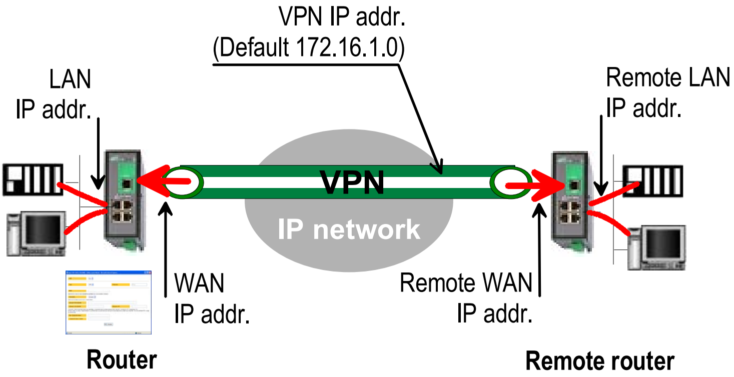
- Select the “**TLS**” VPN type and click “Properties” .

“Port number” & “level 3 protocol” parameters :
Select the port Nr and the type of level 3 protocol used to transport the TLS VPN; UDP will be preferred.

Attention :
The port number value must be different from one used by remote users;

“VPN network address” & “VPN network netmask” parameters :
The TLS VPN server router assigns automatically an IP address to the VPN client router.
That VPN IP address must not be confused with the public IP address assigned to the routers over Internet nor with the private network IP addresses.

Attention :
The VPN IP network address field must be different from the private network IP address field.
The number of VPN addresses cannot be greater than 255; the netmask cannot exceed 255.255.255.0.

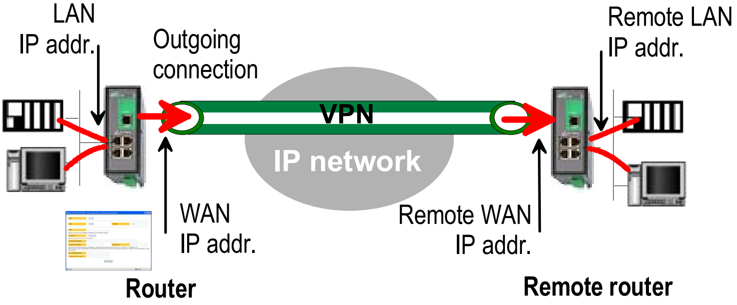


"Connection death time-out" :
This parameter defines the maximum amount of time (in seconds) a VPN connection will stay established before being cleared if no response to the VPN control message has been received from the remote router.

"Repetition time-out" :
A control message (also called Keepalive message) is sent periodically by the VPN server router to make sure that the VPN must be left active.
This parameters sets the amount of time (in seconds) the server will wait for the response before repeating it.

"Encryption algorithm" & "Message digest algorithm" parameters :
That parameters allow to define the encryption and hash algorithms in use.

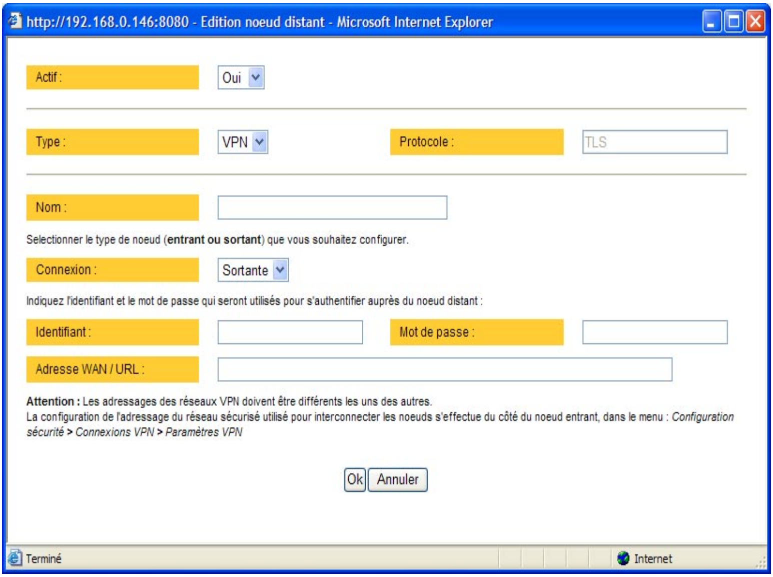
12.3.2 Configuring an outgoing TLS connection



- Select the “**Setup**” menu, the “**network**” menu and then the ‘**VPN connections**” menu.

- Click the “add a connection” button.

Give a name to the connection and select **the “Outgoing” connection direction** option.


http://192.168.0.146:8080 - Edition noeud distant - Microsoft Internet Explorer

Actif : Oui

Type : VPN   Protocole : TLS

Nom :

Selectionner le type de noeud (**entrant ou sortant**) que vous souhaitez configurer.

Connexion : Sortante

Indiquez l'identifiant et le mot de passe qui seront utilisés pour s'authentifier auprès du noeud distant :

Identifiant :   Mot de passe :

Adresse WAN / URL :

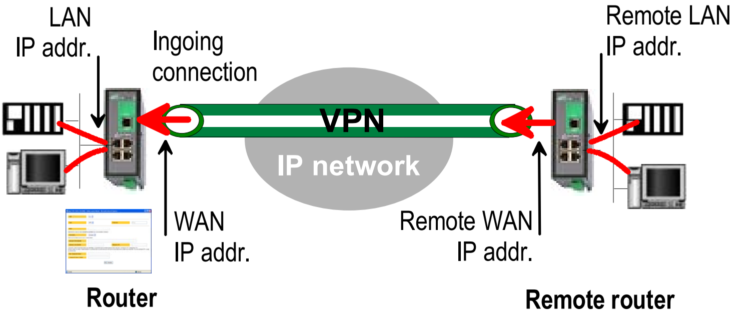
Attention : Les adressages des réseaux VPN doivent être différents les uns des autres.
La configuration de l'adressage du réseau sécurisé utilisé pour interconnecter les noeuds s'effectue du côté du noeud entrant, dans le menu : *Configuration sécurité > Connexions VPN > Paramètres VPN*

“Login & Password” parameter:
Enter the login and password, the router will have to use to authenticate.

“Remote WAN IP address / URL” parameter :
Enter the IP address of the remote router or its DNS name.

“Remote WAN IP address” parameters :
Enter the IP network address and netmask assigned to the remote router over the Internet (public IP address over Internet).

12.3.3 Configuring an ingoing TLS connection



- Select the “**Setup**” menu, the “**network**” menu and then the ‘**VPN connections**” menu.

- Click the “add a connection” button.

Give a name to the connection and select **the “ingoing” connection direction** option.
“Remote router Login” & “Remote router password” parameters :
Enter the login and password of the remote router
The remote router ha to use that login and password to authenticate.

“Remote LAN address” & “Remote LAN netmask” parameters :
Enter the IP network address and netmask assigned to the remote LAN.

“Common name” :
Enter the remote router certificate common name.

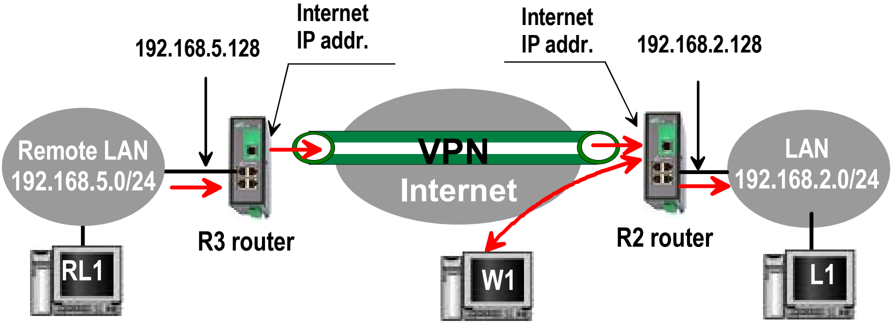
Attention : For ETIC certificates, this field is the Email field

13 Routing functions

13.1 Basic routing function

Once an iP address has been assigned to the R2 router on the LAN interface and another one on the WAN / Internet interface (see drawing hereafter), the IPL-AD2 R2 router is ready to route packets …

> … between devices connected to the remote LAN network like RL1, and devices connected to the LAN network like L1 through a VPN;
>
> … between devices connected to the Internet like W1, and devices connected to the LAN network like L1.

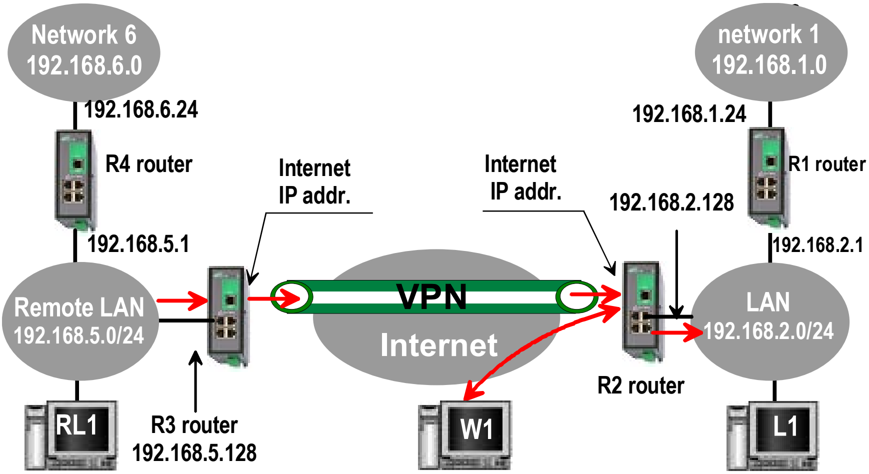


Remark 1 : Firewall rules must be set to authorize WAN to LAN transfer.

Remark 2 : A default gateway address must be entered in each device of the LAN network and the remote .

13.2 Static routes

However, the router R2 is not able to route packets between a device like L1 belonging to the LAN network and a device connected to “network 6” (see the drawing hereafter).



In that case, it is necessary to enter the route to that hidden “network 6”; that route is called a static route.

A static route consists in a table which describes a destination network (IP address and netmask) and the IP address of the neighbour router through which an IP packet to that destination must pass.

Router 2 static routes :

Active	Route name	Destination	Netmask	Gateway
Yes	Network 6	192.168.6.0	255.255.255.0	192.168.5.1
Yes	Network 1	192.168.1.0	255.255.255.0	192.168.2.1

To set a static route,

- Select the “**Configuration**” menu, the “**network**” menu the “**Routing**” menu and then “**Static routes**”.

click the “Add a route” button.

“Destination IP address” & “netmask” parameters :
Enter the destination network IP address and netmask.

“Gateway IP address” parameters :
Enter the Ip address of the gateway through which the IP packets intended for that network must pass.

To set a static route,

- Select the “**Configuration**” menu, the “**network**” menu the “**Routing**” menu and then “**Static routes**”.

- click the “Add a route” button.

13.3 RIP protocol

RIP (**Routing Information Protocol**) is a routing protocol which enables each router belonging to a network to acquire the routes to any subnet.

The principle is as follows :

Routing table
Each router holds a routing table.
Each entry of the table consists in the destination subnet address and the adjacent router address leading to that subnet.

Routing table broadcasting :
Each router broadcasts its table**.**

Routing table update :
Each router updates its own table using the tables received from the other ones.

To enable RIP,

- select the « **Setup**» menu, the “Routing” menu and then the “RIP” menu».
- Select the ‘Enable RIP on LAN interface” and the “Enable RIP on WAN interface” options.

14 Address and port translation

The IPL-AD2 provides the capability to replace the original source IP address and the destination port and IP address in particular situations.

14.1 Address translation (NAT)

That function called NAT applies when a device connected to the LAN wishes to initiate a connection to the WAN or the Internet.

It consists in replacing the IP source address of packets coming from a device connected to the LAN by the WAN IP address of the router.

At the same time, the router will also replace the source port number by a particular port number making possible to route back the responses coming from the Internet to the appropriate device.

To enable the NAT function,

- Select the « Configuration » menu, the “WAN interface” menu, and the « IP protocol menu».
- Tick the checkbox « Activate the address translation (NAT) ».

14.2 Port forwarding

The port forwarding function consists in transferring to a particular device connected to the LAN interface a particular data flow addressed to the IPL-AD2 router on its WAN interface.

That function applies only to the packets addressed to the WAN IP address of the router.

The transfer criteria is the port number; the port number is used as an additional address field :

When a packet is addressed to the IPL-AD2 router with a particular configured port, it is transferred to a particular device connected to the LAN interface.

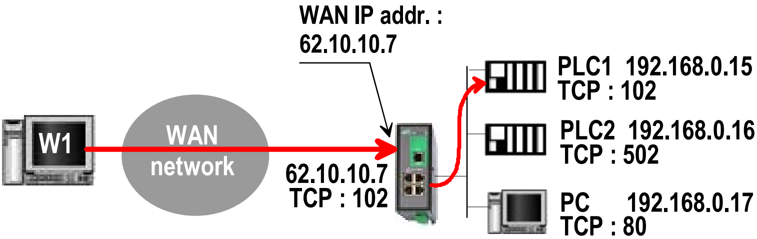
Example :
Let us suppose the PC named "W1" of the WAN network has to send packets to the device PLC1 of the LAN network

Suppose moreover that the addresses of the LAN network cannot be used on the WAN network for any reason.

The solution can be to use the Port forwarding function :

When W1 needs to transmit packets to PLC1, it addresses the packets to the IPL-AD2 router on a chosen and agreed port.

The router checks the packet, replaces the destination address by the Ip address of the device on the LAN interface, and eventually changes the port number.



The port forwarding rule will be

Internet / WAN	LAN translation	
Service	Device	Service
102	192.168.0.15	102
502	192.168.0.16	502
80	192.168.0.17	80

To set the Port forwarding function,

- select the "**network**" menu and then the "**Port forwarding**" menu.
- Click "Add a DNAT" rule.

14.3 Advanced network address and port translation

14.3.1 Principle

This function is available in IPL-AD2-1400B, IPL-AD2-1220B, IPL-AD2-1230B routers only.

That function consists in replacing the source port and IP address and the destination port and IP address of particular packets received by the router on its interfaces according to configured rules.

It applies to all the packets received by the router on any of its two interfaces except to the IP packets contained in a remote user PPTP or TLS connection.

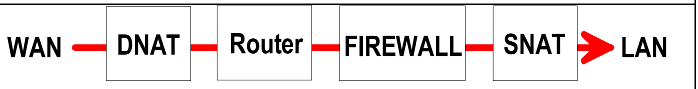
It applies as well to packets the destination address of which is the IPL-AD2 router itself or to packets the destination IP address is a device belonging to the LAN subnet, or to the WAN subnet or to another network.

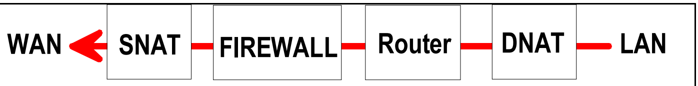
One brings out

the DNAT function which consists in replacing the destination port number and IP address.

the SNAT function which consists in replacing the destination port number and the source IP address.

Because the DNAT and SNAT functions modify the IP addresses of the IP packets processed by the IPL-AD2 router, and because the firewall filters that packets, it is very important to understand in which order that different functions are carried out :

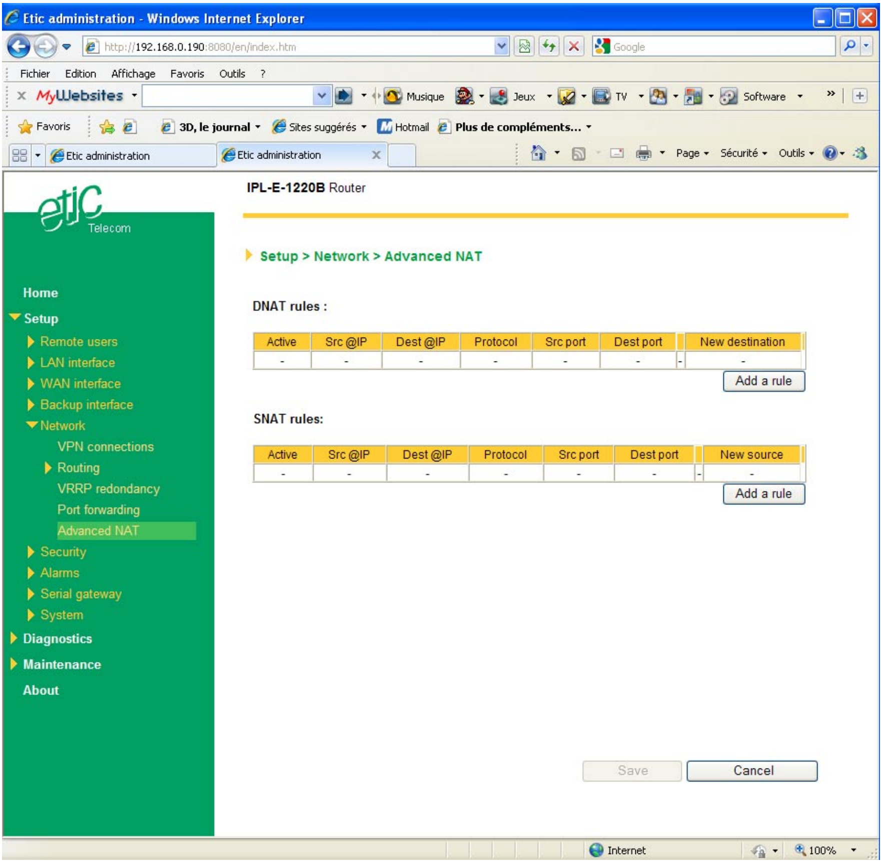
Direction	
WAN to LAN	

LAN to WAN	

14.3.2 Configuration

To set the advanced address translation functions

- select the “**Setup**” menu, “**Network**” , and then the “**Advanced NAT**” menu.



IPL-E-1220B Router

Setup > Network > Advanced NAT

DNAT rules :

Active	Src @IP	Dest @IP	Protocol	Src port	Dest port		New destination
-	-	-	-	-	-	-	-

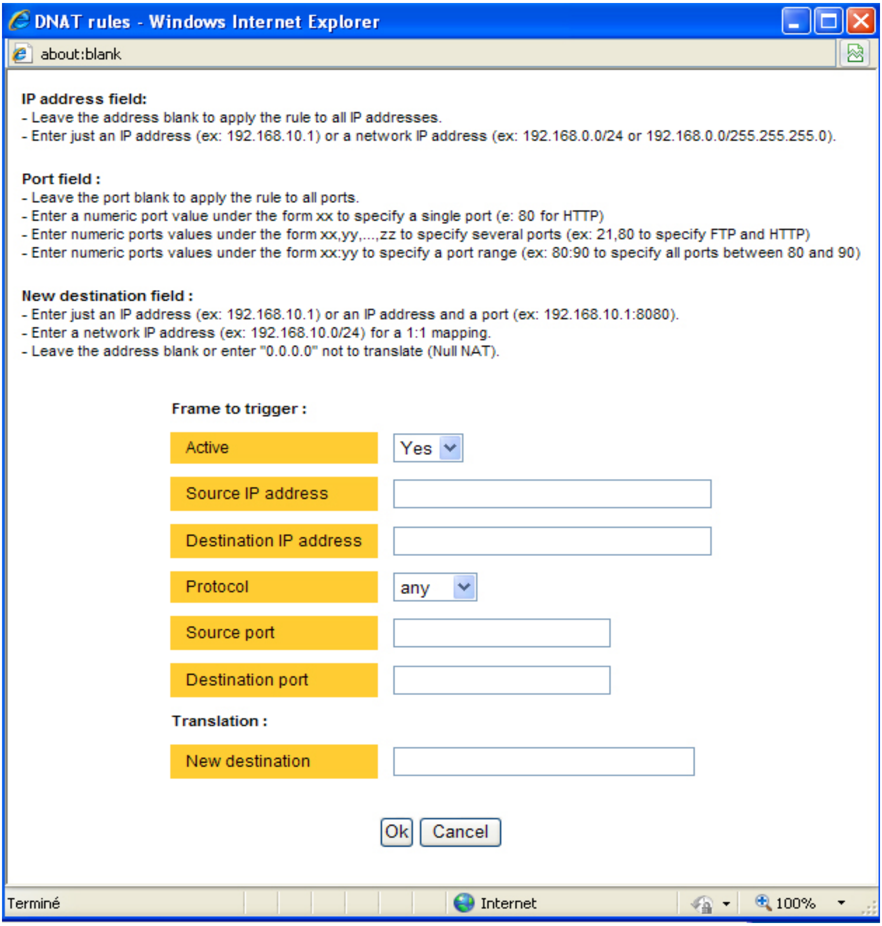
SNAT rules:

Active	Src @IP	Dest @IP	Protocol	Src port	Dest port		New source
-	-	-	-	-	-	-	-

To create a new DNAT rule

- Click "Add a DNAT" rule.
- Select "Yes" to enable the rule.
- Enter the replacement criterion :
  Source IP address & Destination IP address.
  Protocol (TCP, UDP, …)
  Source port & Destination port

- Enter the new destination port number and IP address.



IP address field:
- Leave the address blank to apply the rule to all IP addresses.
- Enter just an IP address (ex: 192.168.10.1) or a network IP address (ex: 192.168.0.0/24 or 192.168.0.0/255.255.255.0).

Port field :
- Leave the port blank to apply the rule to all ports.
- Enter a numeric port value under the form xx to specify a single port (e: 80 for HTTP)
- Enter numeric ports values under the form xx,yy,...,zz to specify several ports (ex: 21,80 to specify FTP and HTTP)
- Enter numeric ports values under the form xx:yy to specify a port range (ex: 80:90 to specify all ports between 80 and 90)

New destination field :
- Enter just an IP address (ex: 192.168.10.1) or an IP address and a port (ex: 192.168.10.1:8080).
- Enter a network IP address (ex: 192.168.10.0/24) for a 1:1 mapping.
- Leave the address blank or enter "0.0.0.0" not to translate (Null NAT).

Frame to trigger :

Active	Yes
Source IP address	
Destination IP address	
Protocol	any
Source port	
Destination port	

Translation :

New destination	

To replace the source IP address & destination port

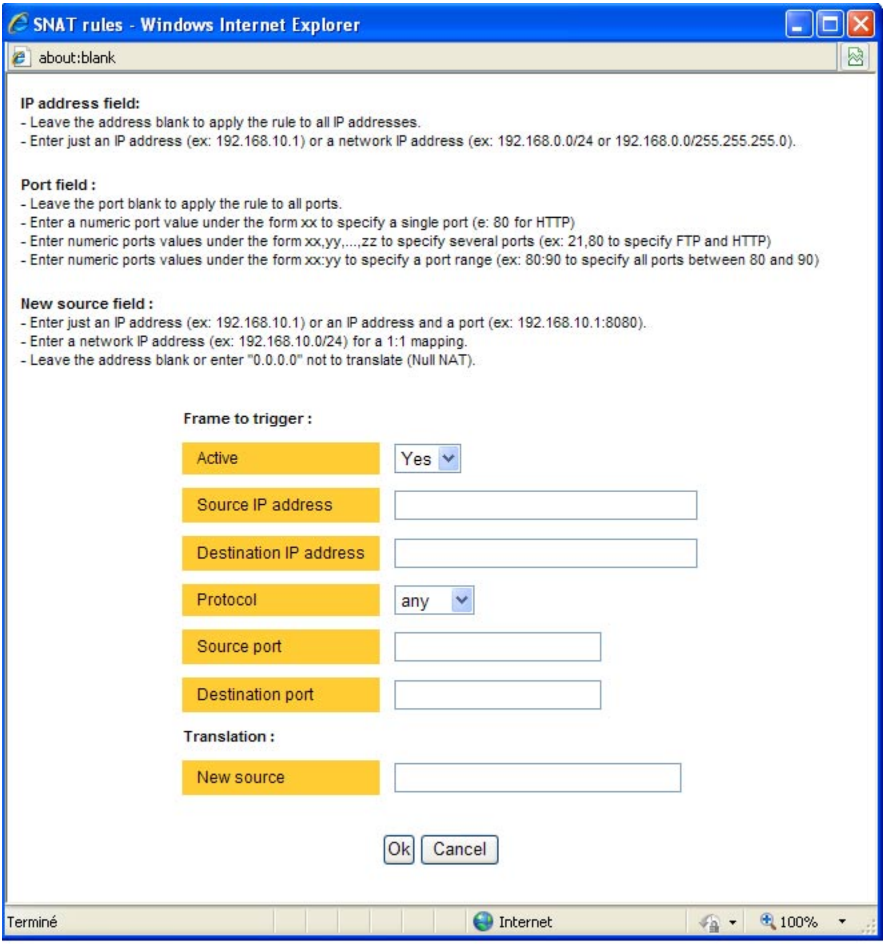
- Click "Add a SNAT" rule.

- Select "Yes" to enable the rule.

- Enter the replacement criterions :

Source & Destination IP address.
Protocol (TCP, UDP, …)
Source & Destination port

- Enter the new source IP address & destination port number



IP address field:
- Leave the address blank to apply the rule to all IP addresses.
- Enter just an IP address (ex: 192.168.10.1) or a network IP address (ex: 192.168.0.0/24 or 192.168.0.0/255.255.255.0).

Port field :
- Leave the port blank to apply the rule to all ports.
- Enter a numeric port value under the form xx to specify a single port (e: 80 for HTTP)
- Enter numeric ports values under the form xx,yy,...,zz to specify several ports (ex: 21,80 to specify FTP and HTTP)
- Enter numeric ports values under the form xx:yy to specify a port range (ex: 80:90 to specify all ports between 80 and 90)

New source field :
- Enter just an IP address (ex: 192.168.10.1) or an IP address and a port (ex: 192.168.10.1:8080).
- Enter a network IP address (ex: 192.168.10.0/24) for a 1:1 mapping.
- Leave the address blank or enter "0.0.0.0" not to translate (Null NAT).

Frame to trigger :

Active	Yes
Source IP address	
Destination IP address	
Protocol	any
Source port	
Destination port	

Translation :

New source	

15 VRRP redundancy

That function is available only in IPL-AD2-1400B, IPL- AD2-1220B, IPL-AD2-1230B routers

15.1 Principle

VRRP is a protocol designed to increase the availability of the default gateway of a subnet.

Thanks to VRRP, a group of two or more routers can service the hosts of one subnet instead of only one usually; only one router of that group actually routes packets; if it fails another one of the group takes its place.

The routers belonging to a VRRP group must be connected to the same Ethernet segment.

VRRP works as follows :

An usual IP address is assigned to each router of the group.

An additional and common IP address, called the virtual IP address is assigned to all the routers of the group. This virtual address is the address which must be stored as the default gateway address in all the host devices belonging to the subnet.

A priority index is assigned to each router of the group. Using that index, the routers of the group can elect a master router; the master router is the one which has the greatest priority code. The other routers are the backup routers.

The master router is the only one to answer to the ARP requests and route actually packets. It uses the virtual IP address and the virtual MAC address If that option has been selected.

In case of failure of the master router, another master router is elected. It replaces the router in failure. It will use the same virtual IP address and the virtual MAC address as the previous master router.

The IPL-AD2 router manages that protocol as well on the LAN and on the WAN interface.

15.2 Configuring VRRP on the LAN interface

To enable and configure VRRP,

- select the “**Setup**” menu, the “**network**” menu and then the “**VRRP” menu**.

«Enable VRRP on the LAN interface» parameters :

Tick that checkbox to enable VRRP on the LAN interface.

«VRRP Id (1-255)» parameter:

Assign an identity code to the routers group between 1 and 255.

The same identity code must be assigned to all the routers of the group.

«Virtual IP address» parameter :

Enter the IP address the elected master router will use to answer to ARP requests.

«Priority (1-255)» parameter :

Assign a priority index to the router

The router which has the greatest index will become the master router.

«Use a virtual MAC address» parameter :

A virtual MAC address can be associated to the virtual IP address.

If that option is selected, the elected master router will answer to ARP requests by using that virtual MAC address.

That MAC address is 00-00-5E-00-01-XX, where XX is the VRRP Id of the group coded in hexadecimal.

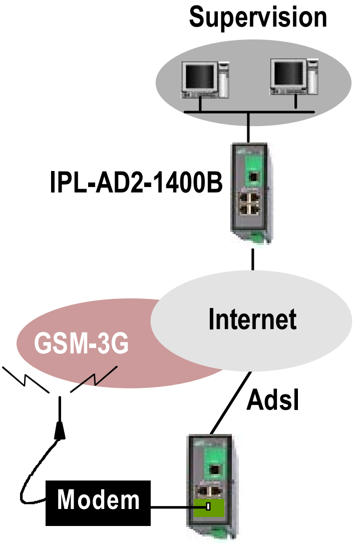
16 GSM-3G wireless backup

IPL-AD2-1201B only.

16.1 Principles

The IPLAD2-1201B router provides a 3G backup function when the ADSL connection fails.

A 3G USB modem must be connected to the USB interface of the IPL-AD2 router.



We recommand to use the TELIT UC864 modem which has been qualified with the IPL-AD2 router.

When the ADSL connection to the Internet provider fails, the IPL-AD2 router routes the data through the 3G network.

The line led associated with the RJ45 ADSL connector is switched off, while the Line led associated to the USB connector switches on to indicate the 3G connection is established.

If a VPN was established through the ADSL line, the IPL-AD2 establishes it again through the 3G network.

Whilst the 3G connection is set, The router tries periodically to set the ADSL line.

A soon as the ADSL line is established, the IPL-AD2 stops transmitting over the 3G wireless network.

Remark :
The backup function works if the ADSL connection uses PPPo Ethernet or PPPo ATM or IPoA (Routed IP over ATM, RFC2684 routed).
But, it does not work if the ADSL connection uses the EoA protocol (Ethernet over ATM RFC2684 Bridged).

16.2 Configuration

To set up the backup function,

- Select the « **Setup**» menu , and then « **Backup interface** », and then the « **Modem** » menu.
- Select the “Enable” checkbox.
- Select the « Telit UC864 » type of modem.
- Select the « GPRS/3G » mode.
- Enter the APN code.

- Select the « **Setup**» menu , and then « **Backup interface** », and then the « **Connection**» menu.

That page allows to setup the PPP connection between the IPL-AD2 router (acting as the PPP client) and the 3G central system (acting as the PPP server) through the air.

« Login» and « Password » parameters :
Enter the login and password associated to the 3G SIM card.

« Authentication» parameter :
Leave the default value (PAP/CHAP)

« Obtain an IP address automatically » checkbox :
Select that checkbox if an IP address is automatically assigned to the router over the 3G network.
This is the usual case.

« Local IP address» and "Remote IP address» parameters :

In particular cases, the IP address of the router on the 3G network and the IP address of the 3G central system are fixed IP addresses and must be entered.

«Obtain DNS servers address automatically» checkbox :

Select that checkbox if the DNS servers addresses are assigned automatically to the router.
This is the usual case.

«Primary DNS server address» and «Secondary DNS server address» parameters:

In particular cases, the DNS servers IP addresses must be entered.

- Select the « **Setup**» menu , and then « **Backup interface** » menu, and then the «**Control**» menu.

«Connect at power-on» parameter :

Select that checkbox.
The IPL-AD2 and the USB 3G modem remain connected to the 3G network.
That checkbox must be selected to enable the backup function.

17 Remote users connections service

The IPL-AD2 provides a full remote user connection function called "RAS" :

- The remote user authenticates using the login, password and eventually a certificate; the router accepts the connection only if the remote user belongs to the user list.
- Individual access rights are automatically allocated to the remote user.
- An IP address belonging to the LAN network is automatically assigned to the remote PC.
- Data are encrypted (TLS and L2TP / IPSec only).
- The connection is logged.
- The IPL-AD2 is compatible with the M2Me_Connect service.

To setup the remote user connection service, the following steps must be carried out :

- Step 1 :

Configure a PPTP or TLS or L2TP / IPSec connection

or select the M2Me_Connect service

- Step 2 :

Complete the user list

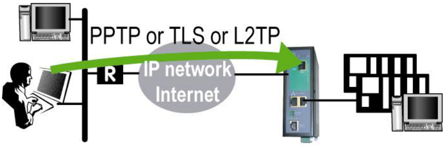
- Step 3 ::

Define the firewall rules to limit the rights of the remote users

18 Remote users connection

18.1 Principles

A remote user connection is a tunnel set between a remote PC and a router providing the RAS function (Remote Access Service), like the IPL-AD2.



A remote user connection provides security and simplicity advantages :

- The remote user is identified with a login in and password or eventually a certificate.

- The data is encrypted (TLS or L2TP).

- An IP address belonging to the local network is automatically assigned to the remote user's PC.

The IPL-AD2 manages PPTP and TLS or L2TP remote connections.

Only one type can be selected. It will apply to all the remote users connections.

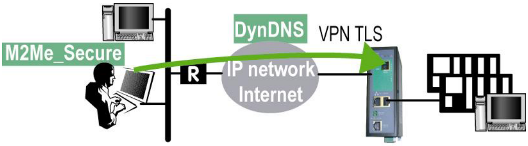
A PPTP is the simplest type of remote user connection; data is not encrypted.
The remote user can be identified only with a login and password.

A TLS connection provides encryption; moreover; the remote user can be identified with a log in and password and with a certificate if necessary.

18.2 Configuring a TLS connection

The M2Me_Secure software provided by ETIC TELECOM is a Windows TLS client software.
Installed on a PC running Windows XP or Seven, M2Me_Secure makes TLS connections from a remote PC to the IPL-AD2 easy; moreover it includes a connection book in such a way one just need a click to connect to a remote site.

We describe hereafter how to configure the router and the M2Me_Secure software to set a TLS VPN between both.



Step 1 : Router configuration

To configure a remote user TLS connection,

- select the “**Setup**” menu, the “**Remote users**” menu and then the “**User list” menu**.
- Select the VPN type “ TLS”.
- Click the “**Properties**” button and set the parameters.

“Port number” & “level 3 protocol” parameters :
Select the port Nr and the type of level 3 protocol used to transport the TLS VPN; UDP will be preferred.

Attention :

The selected port number assigned to the remote users connections must be different from the one used for VPN connections between routers if such VPN connections have been configured.

“Remote User authentication” parameters :

Authentication an encryption can be carried-out with a pre-shared key or a certificate.

If the “Login/password” is selected, the remote user is authenticated with a login and a password.

If the “Login/password and Certificate” value is selected, the remote PC is authenticated with the certificate and the user with a login and password. In that case, the PC certificate must be stored in the user list.

«Encryption algorithm» & «Message digest algorithm» parameters:

Leave the default values

Step 2 : Configure the M2Me_Secure software

For detailed information, refer to the M2Me_Secure manual.

- Click « Menu » and then « New site ». The Site configuration window is displayed.

- Select the « General » tab and enter a site name.

- Select the « Connection » tab; select the option “That site can be reached through the Internet.

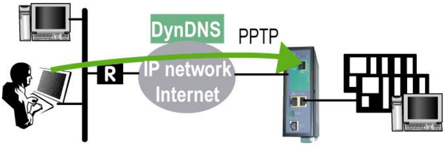
- In the field « Host name or IP address », select the router IP address or DynDNS name or DNS name.

- Select the « Advanced tab » ; select the level 3 protocol (UDP or TCP), the port number and the encryption algorithm.

These parameters must have the same values must in the PC and in the router.

18.3 Configuring a PPTP VPN connection

We describe hereafter how to configure the router and the PC to set a PPTP remote user connection between them.



Step 1 : Router configuration

- select the “**Setup**” menu, the “**Remote users**” menu and then the “**User list” menu**.

- Select the VPN type “ PPTP”.

Remark : The “properties” button allows to modify the authentication protocol; leave the default configuration if the PPTP client is a PC running Windows.

Step 2 : Set a PPTP connection on the PC side.

19 M2Me_Connect service

IPL-AD2-1400B, IPL-AD2-1220B, IPL-AD2-1230B routers only.

19.1 Overview

The M2Me_Connect service simplifies the connection of a remote PC to a machine through the Internet.

It provides a solution when a direct PPTP or TLS connection described before shows itself impossible.

Let us take the example of a machine made of several devices forming a “machine network” and connected to a company network through an IPL-AD2 router.

Suppose an expert wishes to connect to one or several of these devices to help repairing them or to upgrade a firmware.

The simplest solution should be to set a remote connection between the remote PC and the IPL-AD2 through the company network, the existing Internet access in the company, and the Internet.

Several reasons make that connection difficult or impossible, but the main one is a security reason : It is generally not allowed to set an ingoing connection from a PC connected to the Internet towards a device like an IPL-AD2 connected inside a company network.

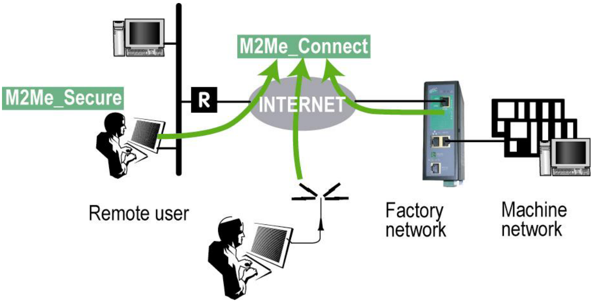
The M2Me_Connect service solves that difficulty :

The PC does not connect directly to the IPL-AD2; both the PC and the router connect to the “M2Me_Connect” service.

Once both parties have been authenticated by the M2Me_Connect service with their own certificate, a TLS VPN is set from end to end from the PC to the IPL-AD2 router.

The remote user identity is checked by the router to verify he or she belongs to the user list stored in the IPL-AD2 router.

Finally, individual access rights are assigned to the remote user depending on his or her identity.



19.2 Configuring a M2Me_Connect connection

Step 1 : Router configuration

- Select the « **Setup**» menu, the « **Remote users** » menu, the “**M2Me_Connect**” menu, and then the “**Connection**” menu.

« Activate » parameter:
Tick the checkbox

“TCP ports” and “UDP ports” parameters :
Select the ports the router must check to set a connection to the M2Me_Connect service.

“Proxy” parameters :
If a proxy server is in charge of filtering IP packets transmitted towards the Internet,
select the “Use a Proxy server” option;
choose either “HTTP” or “SOCK S5”;
Enter the Proxy server address, port number, Login and password.

o Test the connection
Click the “Control” menu, and press the “connect now” button.
Go to the ”Diagnostic” menu, “Network status” menu and then “M2Me”.
When the connection between the router and the M2Me_Connect service is established, the port number and protocol are displayed.

o Deselect the ports number needlessly selected
If too many ports have been selected, the connection delay may be long; it is why we advise to unselect all the ports except the one which has finally been successful.

Step 2 : Configuring the M2Me_Secure software

- Click « Menu » and then « New site ». The Site configuration window is displayed.
- Select the « General » tab and enter a site name.

- Select the « Connection » tab; select the option “That site can be reached through the Internet and the “M2Me_Connect” option.

- Enter the product key of the router; it can be pasted from the “About” menu of the router.

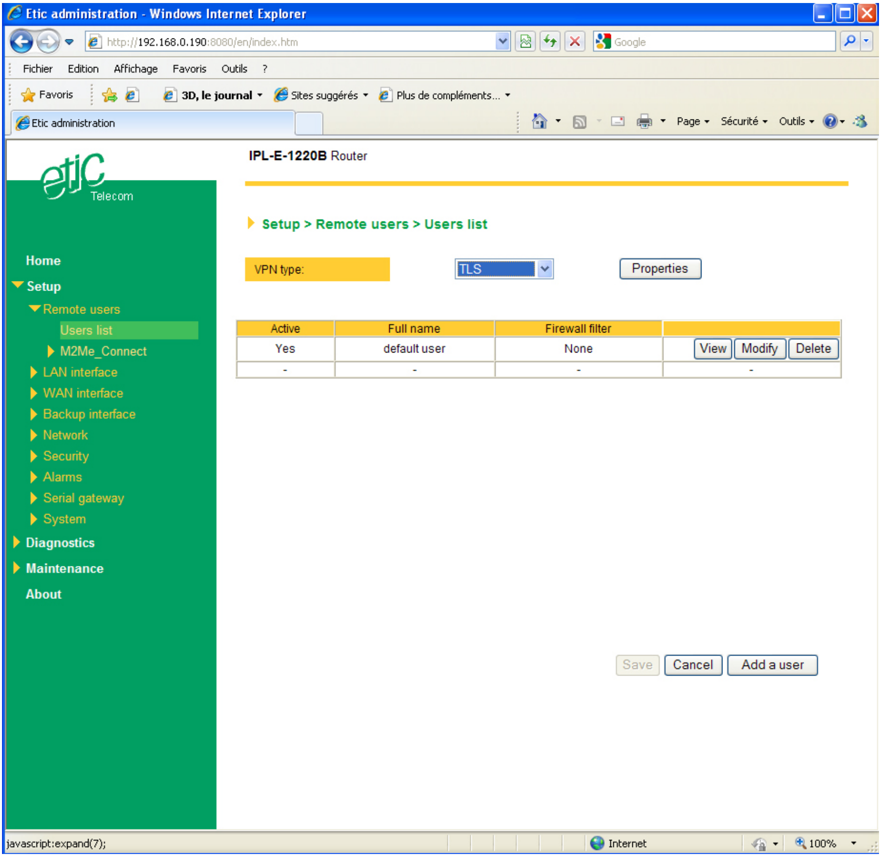
20 Users list

The user list registers 25 authorised remote users forms.

Each user form stores the identity of the user (Login and password), his email address to send alarm emails and the filter assigned to him.

To display the user list,

- select the "**Setup**" menu, the "**Remote users**" menu and then the "**User list"** menu.



IPL-E-1220B Router

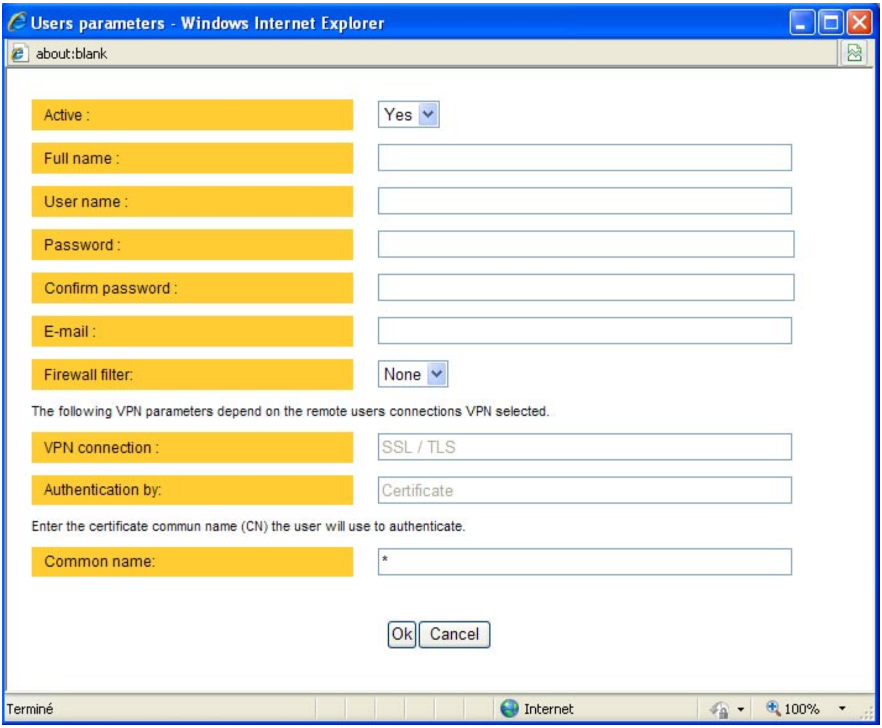
Setup > Remote users > Users list

VPN type: TLS

Active	Full name	Firewall filter	
Yes	default user	None	View Modify Delete
-	-	-	-

Attention :
Coming from factory, a default user is registered; his login is **admin** and the password is also **admin**. After the test phase, we advise to modify these login and password.

To add a user form



Users parameters - Windows Internet Explorer

about:blank

Active :	Yes
Full name :	
User name :	
Password :	
Confirm password :	
E-mail :	
Firewall filter:	None

The following VPN parameters depend on the remote users connections VPN selected.

VPN connection :	SSL / TLS
Authentication by:	Certificate

Enter the certificate commun name (CN) the user will use to authenticate.

Common name:	*

- Click the “add a user ” button

“ Active (value Yes or NO)” parameters :
Select “No” if you want to prevent the user to access the network.
Select “yes” to authorize the user to access the network.

“Full name” parameters :
It is the name displayed in the user list.

“Login” & “password” parameters :
The login and the password will have to be entered by each user at the beginning of the remote connection.

“E-mail” parameters :

The IPL-AD2 will send an email to that address in two situations :
Alarm email : the IPL-AD2 sends an alarm email to the defined user If the input 1 is closed or opened (if that option has been set).

Internet connection email : Once connected to the Internet, the IPL-AD2 will send to the demanding user an email containing the dynamic IP @ assigned to the IPL-AD2 by the provider. (See OPERATION chapter).

“Firewall filter” parameters :

Select a filter in the list.
A filter defines a domain of the local network.
Thus, once assigned to a user, a filter limits his or her access rights.

21 Configuring the firewall

21.1 Overview

The firewall filters IP packets between the WAN and the LAN interface of the IPL-AD2 router. It is divided in 3 particular filters :

- **The remote users** filters

The function of the remote users filters is to limit the IP domain an authenticated remote user can reach when he connects to the IPL-AD2 router through the Internet.

The remote users filters filter the destination IP address and port number of the IP packets included inside à PPTP or TLS or L2TP remote user connection.

Thus the IP addresses checked by the remote users filters are LAN IP addresses.

25 remote users filters can be created and assigned individually to each of the users declared in the user list.

The source IP address of the packets is not checked by the remote users filters because the filters apply to the remote users connections according the login and password of the remote user checked when the remote user connection is set.

- **The main filter**

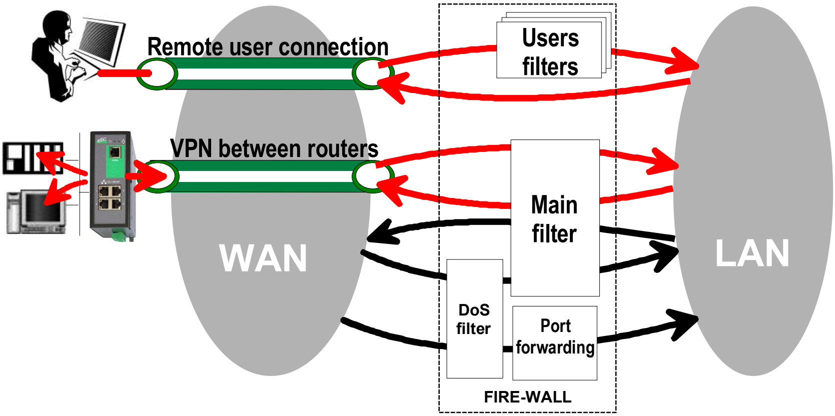
It filters IP packets whether carried inside one of the VPNs or outside a VPN.
The main filter checks source and destination IP addresses and the source and destination ports.

The main filter does not check the IP packets included in a remote user connection. That packets are checked by the remote users filter.

The main filter does not check the IP packets defined in the “Port forwarding” table. That packed are directly forwarded to the defined device (see Port forwarding).

- **The deny of service filter** is made to usual attacks coming from the Internet. That filter cannot be configured.

The firewall of the IPL-AD2 firewall can thus be represented by the drawing hereafter :



21.2 Main filter

The main filter applies to all the IP packets except to the ones included in remote users connections.

To recognize a TLS remote user connection, the router detects the port number.

21.2.1 Main filter Overview

- **Main filter structure**

For a better organisation, the main filter is divided in two tables; both having the same structure.

The “VPN” filter : It filter the packets transmitted inside the VPNs.
The “WAN” filter : It filters the packets transmitted outside the VPNs

Each of that two filters is made of

a filter policy
and
a filter table each line of which is a filter rule

- **Main filter default policy**

The default policy is the decision which will be applied if a packet does not match any of the rules of the filter.

The WAN to LAN and the LAN to WAN traffic are regarded separately because the decision can be opposite for a packet coming from the WAN or coming from the LAN :

WAN to LAN : The default policy can be “Accept” or “drop”.

LAN to WAN : The default policy can also be “Accept” or “drop”.

For instance, if the default policy assigned the WAN to LAN traffic is “drop”, it means that an IP packet which does not match any of the rules of the main filter will be rejected.

- **Main filter table**

The main filter is a table, each line being a rule.

Each rule of the filter is composed a several fields which defines a particular data flow and another field which is called the action field.

The fields which define the data flow are :

Direction (« WAN to LAN » or « LAN to WAN »),
Protocol (TCP, UDP…),
IP@ & port number, source & destination.

The Action field can take two values

Accept : To authorize the data flow to be forwarded to the router interface.
Drop : To drop the packet which matches the rule.

- **How does the main filters works**

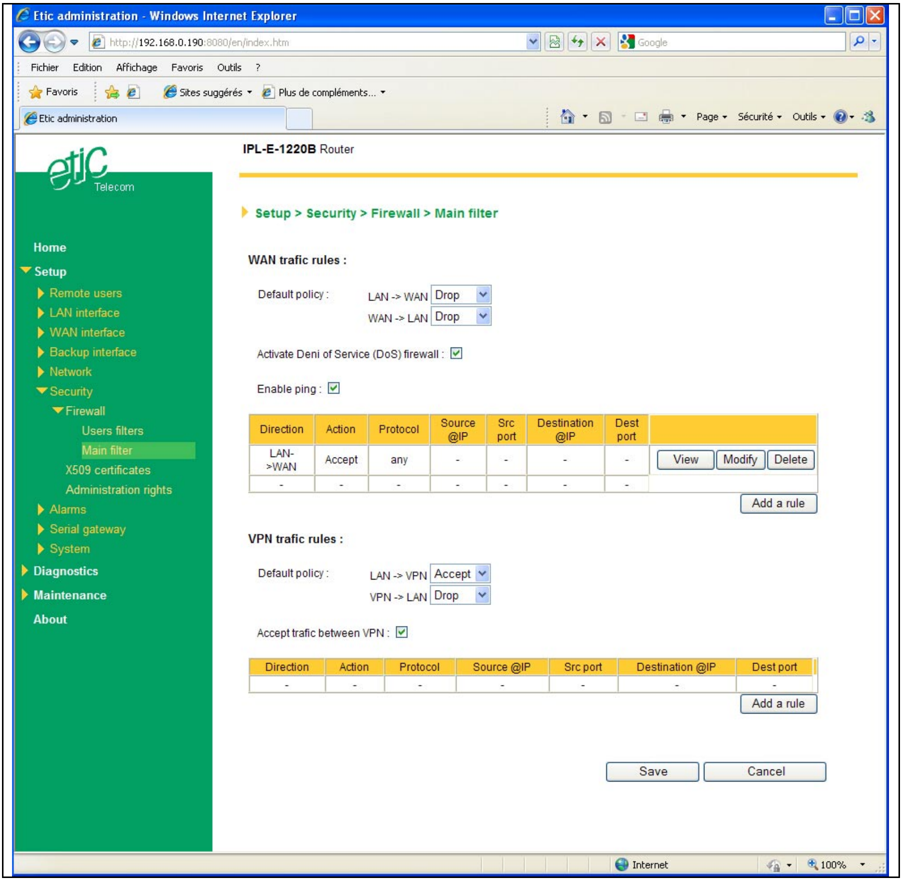
When the firewall receives a packet, it checks if it matches the first rule..
If it does, the decision is applied to the packet according to the “Action” field.

If it does not, the firewall checks if it matches the second rule; and so on.

If the packet does not match any of the rules of the table, the default policy is applied to the packet (drop or reject).

21.2.2 Configuring the main filter

Select the “**Security**” menu and then “**Firewall**” and “**Main filter**”.



IPL-E-1220B Router

Setup > Security > Firewall > Main filter

WAN trafic rules :

Default policy : LAN -> WAN Drop
WAN -> LAN Drop

Activate Deni of Service (DoS) firewall : ☑

Enable ping : ☑

Direction	Action	Protocol	Source @IP	Src port	Destination @IP	Dest port	
LAN->WAN	Accept	any	-	-	-	-	View Modify Delete
-	-	-	-	-	-	-	

Add a rule

VPN trafic rules :

Default policy : LAN -> VPN Accept
VPN -> LAN Drop

Accept trafic between VPN : ☑

Direction	Action	Protocol	Source @IP	Src port	Destination @IP	Dest port
-	-	-	-	-	-	-

Add a rule

Save Cancel

The “Main filter” page is divided in two parts :

WAN traffic rules :
The first part, entitled “WAN” traffic rules, is made to define how the IP packets **not carried in a VPN,** have to be filtered.

VPN traffic rules :
The second part, entitled “VPN traffic rules” allows to define how the IP packets **carried inside the VPNs** have to be filtered.

Configure successively the WAN traffic rules using the same method.

Step 1 : Select the default policy

"LAN to WAN" parameter :
That parameter sets what the filter will decide if an IP packet coming from the LAN does not match any f the rules of the filter :
If the value "Accept" is selected, the IP packet will be transmitted to the VPN.
If the value "Drop" is selected, the IP packet will be rejected.

"WAN to LAN" parameter :
That parameter sets what the filter will decide if an IP packet coming from the WAN does not match any f the rules of the filter :
If the value "Accept" is selected, the IP packet will be transmitted to the LAN.
If the value "Drop" is selected, the IP packet will be rejected.

The cautious default policy is to choose the value "Drop"; at the opposite, if the value "Accept" is selected, a packet which does not match any of the rules of the filter is transmitted.

Step 2 : Add a rule to the filter

Click the "add a rule" button.

"Direction" parameter :
Select the direction of the data flow to which the rule applies.

"Action" parameter :
Select the value "Accept" if the IP packet has to be transmitted in the selected direction.
Select the value "Drop" if the IP packet has to be rejected.

"Protocol" parameter :
Select the level 3 protocol concerned.

"Source IP address" & "Source port" parameters :
Enter the value of the source IP address and the source port number.
It is possible to enter a range of source IP addresses and not a single IP address by selecting a netmask value from 1 to 32; It is the number of binary 1 of the netmask; for instance, the value 24 means 255.255.255.0; the value 16 means 255.255.0.0.

”Destination IP address” & “destination port” parameters :
Enter the value of the destination IP address and the destination port number. Select the netmask value.

21.3 Remote users filters

A remote user filter applies to the IP packets received inside a remote user connection.

25 remote user filters can be configured and assigned individually to each of the users declared in the user list.

A remote user filter is a table of destination port numbers and IP addresses belonging to the LAN network.

Once a remote user is connected to the IPL-AD2 router, the router applies the filter assigned to him (see the remote user form).

According to his identity (Login and password, he will thus only access to the IP domain defined by the filter.

Example :

Filter name : Access to the device PLC1 (html and modbus)		
Filter policy : All is forbidden except what we specify		
Rules list		
Action	Device	Service
Allow	PLC1 192.168.0.12	80
Allow	PLC1 192.168.0.12	Modbus 502

A filter must be assigned at least to one user to become enabled.

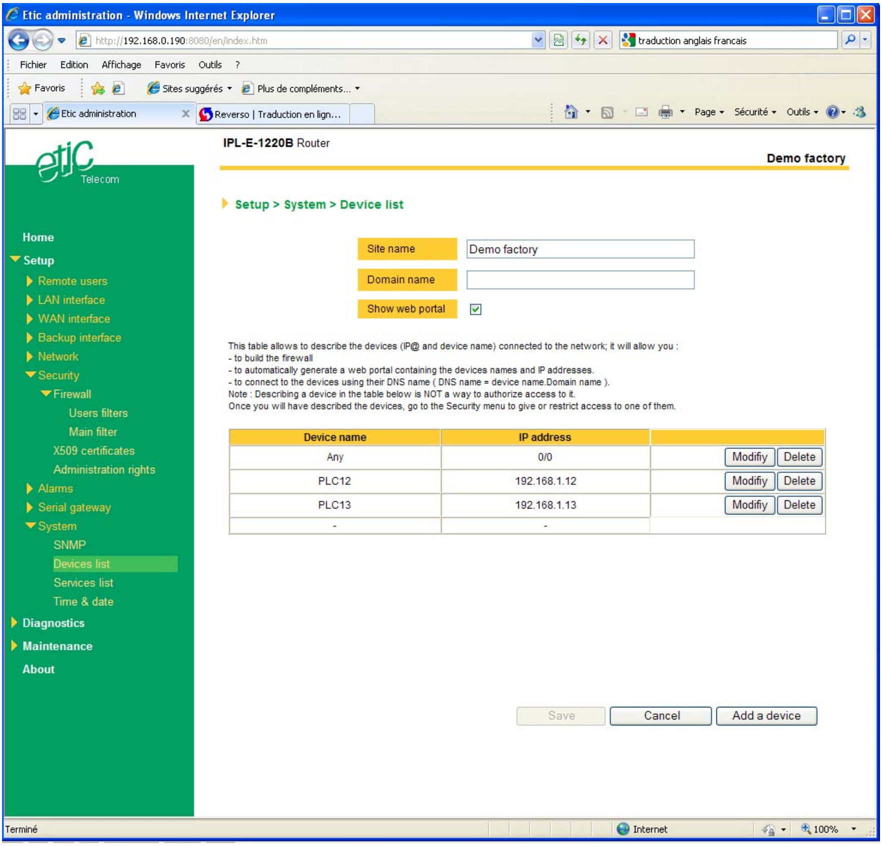
Step 1 : Complete, if necessary, the list of services

Remark : *The main services (html, ftp, modbus) are available from factory; for that reason, most of the time, that step can be skipped.*

- Select the menu “system” and then “service list” The list of TCP ports is displayed.
- Click « add a service ».
- Enter the label of that the new service, assign a protocol (udp, tcp, icmp) and a port number.
- Save. The list is updated.

Step 2 : Enter the list of devices of the LAN network

- Select the «System» menu, then «Devices list».
  The list of the devices of the LAN network is displayed.



IPL-E-1220B Router

Demo factory

Setup > System > Device list

Site name	Demo factory
Domain name	
Show web portal	☑

This table allows to describe the devices (IP@ and device name) connected to the network; it will allow you :
- to build the firewall
- to automatically generate a web portal containing the devices names and IP addresses.
- to connect to the devices using their DNS name (DNS name = device name.Domain name).
Note : Describing a device in the table below is NOT a way to authorize access to it.
Once you will have described the devices, go to the Security menu to give or restrict access to one of them.

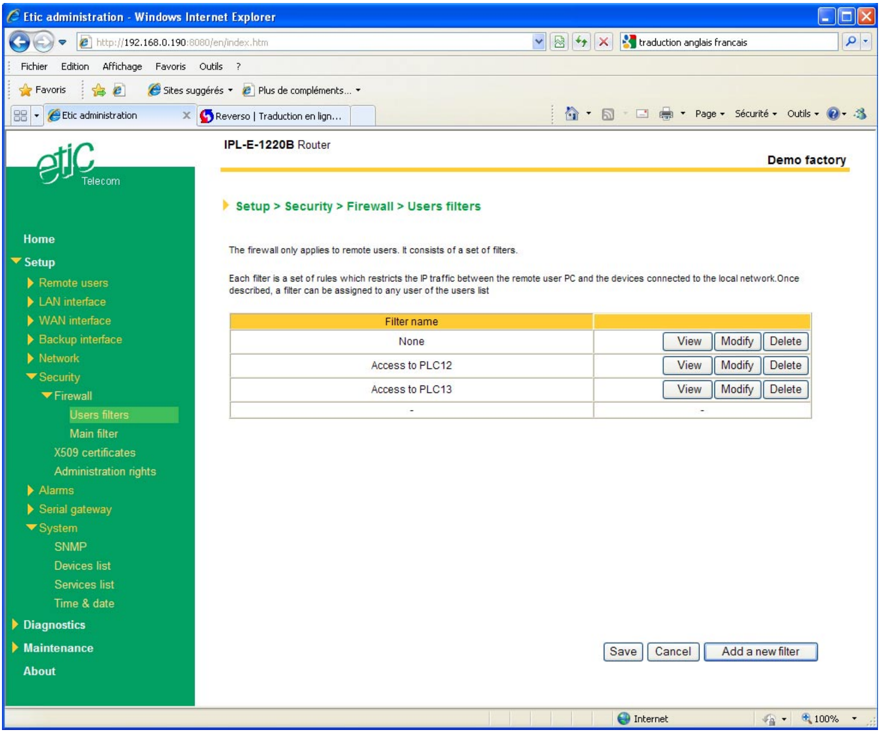
Device name	IP address	
Any	0/0	Modifiy Delete
PLC12	192.168.1.12	Modifiy Delete
PLC13	192.168.1.13	Modifiy Delete
-	-	

Save Cancel Add a device

- Click « add a device ».
- Assign a label and an IP address to the device and click OK.

Step 3 : Build a remote user filter

- Select the « security» menu, then « firewall» and then «Filter list» The users filters list is displayed.



IPL-E-1220B Router

Demo factory

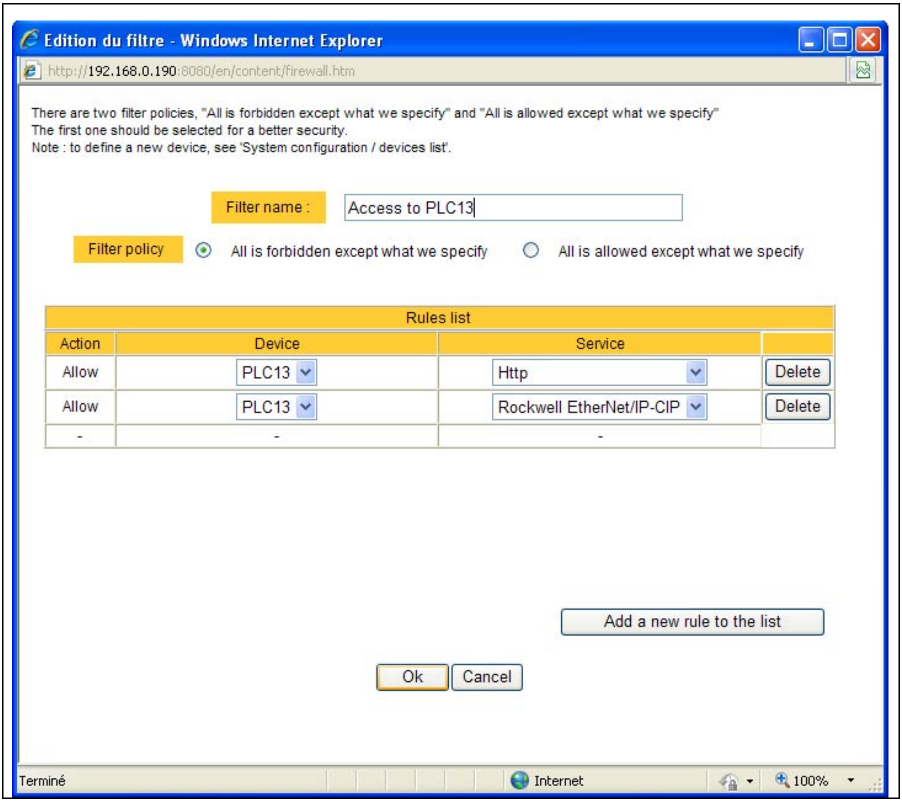
Setup > Security > Firewall > Users filters

The firewall only applies to remote users. It consists of a set of filters.

Each filter is a set of rules which restricts the IP traffic between the remote user PC and the devices connected to the local network.Once described, a filter can be assigned to any user of the users list

Filter name	
None	View Modify Delete
Access to PLC12	View Modify Delete
Access to PLC13	View Modify Delete
-	-

- Click « add a new filter ».



Edition du filtre - Windows Internet Explorer
http://192.168.0.190:8080/en/content/firewall.htm

There are two filter policies, "All is forbidden except what we specify" and "All is allowed except what we specify"
The first one should be selected for a better security.
Note : to define a new device, see 'System configuration / devices list'.

Filter name : Access to PLC13

Filter policy ● All is forbidden except what we specify ○ All is allowed except what we specify

Rules list			
Action	Device	Service	
Allow	PLC13	Http	Delete
Allow	PLC13	Rockwell EtherNet/IP-CIP	Delete
-	-	-	

- Assign a name to the new filter.
- Choose the policy ; « All is forbidden except what we specify » is the advised policy.
- Click « add a new rule to the list ».
- Select a device among the ones which have been stored and a service (also called port).
- Add other rules if necessary.
- Click OK when the filter is complete ; the updated filter list is displayed.

Step 4 : Assign a filter to each user

- Select the « Remote user» and then « User list ».
- Select a user to which you want to assign a filter ; and click modify ; the user window is displayed.

Assign a filter to the user ; click OK and save.

22 Serial to IP gateway

The IPL-AD2 features two serial ports.

A serial gateway can be assigned to each port .

If the same type of gateway is assigned to both serial ports, the UDP or TCP port numbers must be different.

The gateways listed below are provided :

Modbus client or server (i.e. master or slave)
To connect several serial modbus slaves to several IP modbus clients.
Or to connect a serial modbus master to an IP modbus server.

RAW TCP server or client :
To connect 2 serial devices through an IP network.

Telnet :
To connect a Telnet terminal to the RAS.

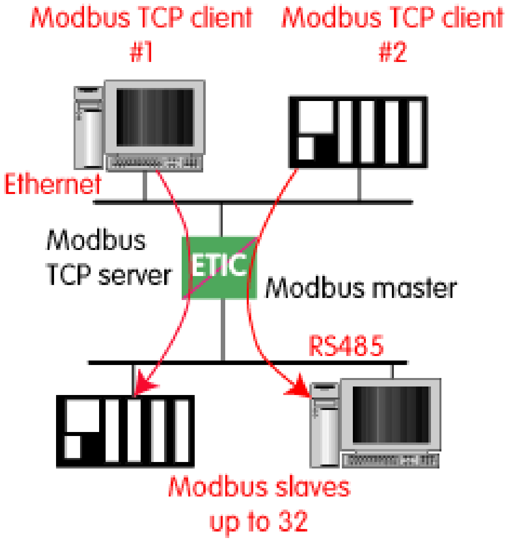
RAW UDP :
To exchange serial data between several serial and IP devices, through an IP network, using a table of IP addresses..

Unitelway slave :
To connect a serial unitelway master to an IP network.

22.1 Modbus menu

22.1.1 Modbus server gateway

This gateway allows to connect asynchronous modbus slaves to the serial interface of the IPRS.



- Select the modbus menu and then modbus server and enable the modbus server gateway and set the parameters as follows :

“Port selection” parameter :
Select the serial port COM 1 or COM2.
If the modbus server gateway is assigned to one serial COM port, it cannot be assigned to the other one.

« ASCII / RTU protocol » parameter:
Select the right option

“Proxi” parameter:
Enable the proxi option if you wish to avoid to frequent requests on the RS232-RS485 interface.

“Cache refreshment period” parameter:
Select the period at which the gateway will send request to the slaves PLC.

“Timeout waiting for the answer” parameter:
Set up the timeout the gateway has to wait for the answer of the modbus slave answer.

“Local retry” parameter :

Set up the number of times the gateway will repeat a request before declaring a failure.

“Inter-character gap” parameter :

Set up the maximum delay the gateway will have to wait between a received character of a modbus answer packet and the following character of the same packet.

“Modbus slave address” parameter:

Choose “specified by the modbus TCP client” , if the address of the slave PLC must be decoded by the gateway from the modbus TCP packet coming from the client.
Otherwise, specify the modbus address of the slave PLC; in that case only one slave can be connected to the RS232 serial interface.

“TCP inactivity Timeout” parameter :

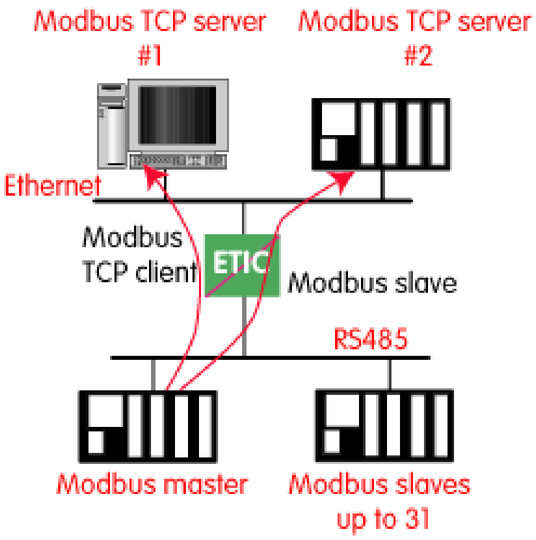
Set the time the gateway will wait before disconnecting the TCP link if no characters are detected.

“TCP port number” parameter :

Set the port number the gateway has to use.
If the Raw TCP client gateway is assigned to both serial COM ports, the TCP port numbers must be different on each port.

22.1.2 Modbus client gateway

This gateway allows to connect a serial modbus master to the serial interface of the IPRS.



- Select the modbus menu and then “modbus client” menu; enable the “modbus client” gateway and set up the parameters as follows :

“Port selection” parameter :
Select the serial port COM 1 or COM2.
If the modbus server gateway is assigned to one serial COM port, it cannot be assigned to the other one.

« ASCII / RTU protocol » parameter :
Select the right option

“Inter-character gap” parameter :
Set up the maximum delay the gateway will have to wait between a received character of a modbus answer packet and the following character of the same packet.

“TCP inactivity Timeout” parameter :
Set the time the gateway will wait before disconnecting the TCP link if no characters are detected.

“TCP port number” parameter :
Set the TCP port number the gateway has to use.

“IP address” parameter :
The modbus client gateway allows to transmit modbus requests from the serial modbus master device to any modbus slave device, more precisely called “ modbus server”, located on the IP network.

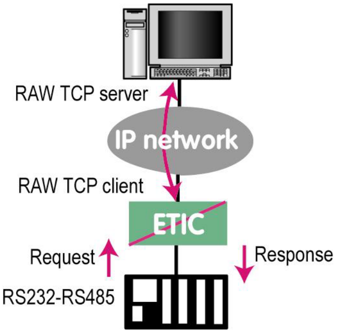
To assign an IP address to each modbus slave device with which the serial master device needs to communicate, click the “add a link” button; Assign an IP address in front of each modbus slave address with which the serial master device will have to communicate.

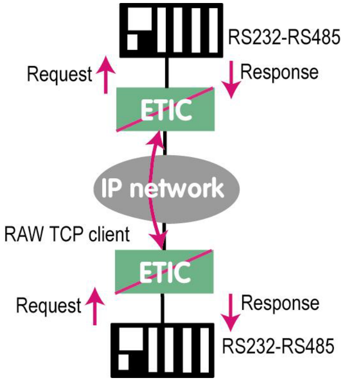
22.2 RAW TCP gateway

22.2.1 Raw client gateway

The RAW client gateway can be used if a serial “master” device has to send requests to one slave device (also called server) located on the IP network.

The server can be either an ETIC gateway or a PC including a software TCP server.





- Select the “transparent” and then the “raw client COM1” or the “raw client COM2” menu .

- Enable the raw client gateway; and set up the parameters as follows :

“RS232/485 input buffer size” parameter :
Set up the maximum length of an asynchronous string the gateway will store before transmitting it to the IP network.

“Timeout of RS232/485 end of packet” parameter :
Set up the delay the gateway will wait before declaring complete a string received from the asynchronous device.
Once declared complete, the gateway will transmit the string to the IP network.

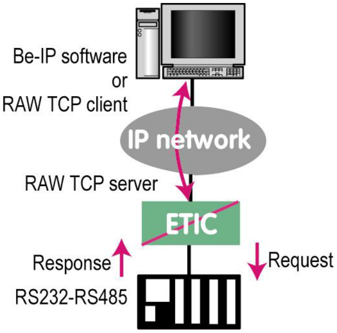
“TCP inactivity Timeout” parameter :
Set the time the gateway will wait before disconnecting the TCP link if no characters are detected.

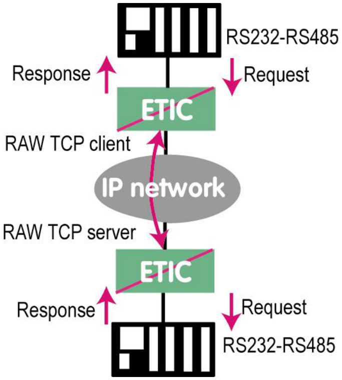
“TCP port number” parameter :
Set the port number the gateway has to use.
If the Raw TCP client gateway is assigned to both serial COM ports, the TCP port numbers must be different on each port.

“Raw server IP address” parameter :
The raw client gateway is able to communicate with a raw server gateway. Assign an IP address to define the destination gateway.

22.2.2 Raw server gateway

That gateway can be used if a serial slave device has to answer requests coming from devices located on the IP network and acting like a master (also called TCP client).





- Select the “transparent” and then the “raw server COM1” or the “raw server COM2” menu.

- Enable the raw server gateway and set up the parameters as follows :

“RS232/485 input buffer size” parameter :
Set up the maximum length of an asynchronous string the gateway will store before transmitting it to the IP network.

“Timeout of RS232/485 end of frame” parameter :
Set up the delay the gateway will wait before declaring complete a string received from the asynchronous device.
Once declared complete, the gateway will transmit the string to the IP network.

“TCP inactivity Timeout” parameter :
Set up the time the gateway will wait before disconnecting the TCP link if no characters are detected.

“TCP port number” parameters :
Set up the port number the gateway has to use.
If the Raw TCP server gateway is assigned to both serial COM ports, the TCP port numbers must be different on each port.

22.3 RAW UDP gateway

22.3.1 Overview

The RAW UDP gateway enables you to connect together a group of serial or IP devices through an IP network.

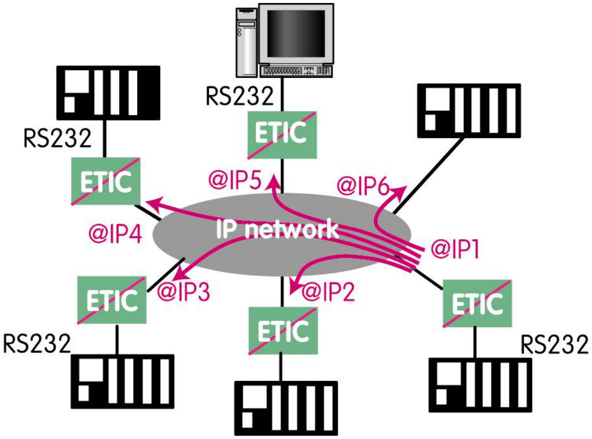
The group can include IP devices if they have the software pieces able to receive or transmit serial data inside UDP.

Serial data transmitted by each device is transmitted to all other serial devices through the IP network.

A table of IP destination gateways is stored in each IPL-AD2 belonging to the group.

The serial data is encapsulated in the UDP protocol.

The UDP datagram is sent to each destination IP address stored in the table.



22.3.2 Configuration

- Select the “gateway” menu and then the “Transparent” menu and then click “RAW UDP”.

- Select the “Activate” option.

« Serial input buffer size” parameter (value 1 to 1024) :
Sets the maximum size of an UDP datagram.

“End of frame time-out” parameter (value 10 ms to 5 sec) :
Sets the delay the gateway will wait before sending the UDP datagram towards the IP network when no characters are received from the serial interface.

«UDP port number» parameter :
Sets the UDP port number.
If the Raw UDP gateway is assigned to both serial COM ports, the UDP port numbers must be different on each port.

“IP addresses of the destination devices » table :
This table stores the IP addresses of the gateways to which the serial data, encapsulated inside UDP, have to be sent.
A different UDP port number can be entered for each destination IP address.

23 Advanced functions

23.1 Adding a certificate

Coming from the factory, the IPL-AD2 router includes a certificate delivered by ETIC TELECOOMUNICATIONS acting as a certification authority.

That certificate can be used to set a VPN between two routers.

Two IPL-AD2 routers can set a VPN with one another using certificates only if the certificates have been provided by the same authority.

Additional X509 certificates, provided by ETIC Telecommunications or not, can be downloaded into the router.

To import a new certificate, the file extension can be PKCS#12 with a password or PEM.

Even if more than one certificate have been downloaded into the IPL-AD2 router, one certificate can be used for all the connections.

23.2 Alarms

23.2.1 SNMP

The IPL-AD2 router is able to send snmp traps when alarms occur.

”**Activation” parameter :**
If that option is selected, the router will send an SNMP trap if an alarm is detected.

“SNMP network management IP address” parameters :
Enter the IP address of the management platform

“SysName” & “SysLocation” parameters :
That fields allow to identify the source device.
Example :
Sysname : etic
Syslocation : France

“Product start-up” parameter :
If that option is selected, the router will send an SNMP trap each time it will connect to the Internet

23.2.2 Digital output alarm

If an alarm occurs, the router will open the digital output..

The causes which make the output to open cane be either the ADSL disconnection, power input 1 failure, power input 2 failure.

23.2.3 E-mail alarm

When the digital input is closed or opened, an email can be transmitted to one of the users of the users list.

To set that function select the “Alarm” menu and click “email”.

“Enable the alarm email” parameter :
Select this option if you want an email to be sent to a user when the digital input 1 is set ON or OFF.

“Alarm launched on event” parameter :
If the option OPEN is selected, the alarm will be sent each time the digital input will be opened.
If the option CLOSED is selected, the alarm will be sent each time the digital input will be opened.
If the option BOTH is selected, the alarm will be sent each time the digital input will be opened or closed.

”Hold time” parameter :
Select the time the input has to stay in its alarm state to be taken into account.

“Alarm destination” parameter :
Select the user to whom the email must be sent.

“Text to send” parameter :
Enter the email text.

23.3 Configuring the web portal

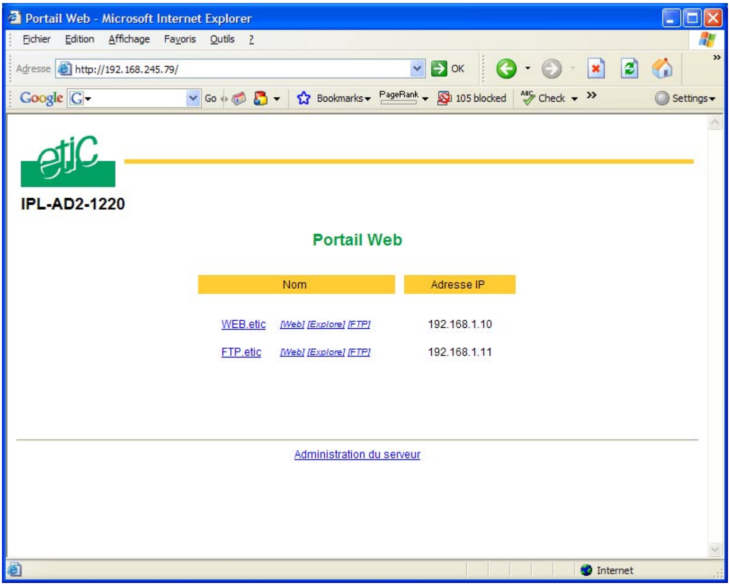
The web portal in an html page; it displays a list of devices connected to the LAN. Each line of the list is made of the device name, its IP address and three links :

The html link : To go directly to the web server of the associated machine.

The « explore » link : To explore the HD of the associated machine, if it is a Windows machine.

The « ftp » link : To explore the files of the associated device.

If the we portal option has been selected (see below), the web portal page is displayed when the remote user launches the navigator and enters the Ip address assigned to the IPL-AD2 router. In that case, the administration server, usually can be displayed at the same address but at the port number 8080 instead of 80 when the web portal page option is not selected.


Portail Web - Microsoft Internet Explorer
Fichier Edition Affichage Favoris Outils ?
Adresse http://192.168.245.79/
OK
Google G Go Bookmarks PageRank 105 blocked Check Settings
Internet

IPL-AD2-1220

Portail Web

Nom		Adresse IP
WEB.etic	[Web] [Explore] [FTP]	192.168.1.10
FTP.etic	[Web] [Explore] [FTP]	192.168.1.11

Administration du serveur

23.4 Configuring the DNS server

For domain names resolution, the IPL-AD2 can behave like a domain name server or a domain name relay.

DNS server :
A domain name server is a networking device which is able to associate a label (etictelecom.com for instance) with an IP address.

That function allows a client device to send a request to a network equipment referring to a domain name as if it was the actual IP address of the destination device.

The IPL-AD2 router is able to resolve any domain name composed with the name of one of the devices entered in the devices list followed the site name which is entered at the top of the devices list.

DNS relay :

The IPL-AD2 router behaves also like a DNS relay; any DNS request it receives from the LAN, which cannot be resolved because the device is not registered in the devices list, will be transferred to the internet to be resolved.

That function can be carried out only if the IPL-AD2 IP address is pointed out as the main DNS server of the devices of the LAN.

That function is efficient in particular when a device connected to the LAN has to send emails through the Internet.

.

1 Diagnostic

The html server provides extended diagnostic functions.

Select the Diagnostic menu and then the appropriate sub-menu.

- **Log sub-menu:**

The log displays the last 300 dated events :

ADSL, VPN and users connections and disconnections,
power on,
Serial gateway events.

- **Network status sub-menu and then status sub-menu :**

That screen displays the current status of the LAN interfaces and of the Internet connection :

LAN interfaces :

That part of the page shows the data of the LAN interface :

MAC address,
Ethernet mode (10 /100, half or full),
IP address.

Internet connection :

That part of the page shows the data of the Internet interface :

ADSL data rates,
Internet IP address,
DNS IP address.

The “View statistics” button gives access to the ADSL statistics windows; that windows shows

the reception signal attenuation,
the Signal to noise margin (SNR margin),
G821 error rates indicators.

- **VPN sub-menu**

That menu displays the table of the VPN (remote user connections and remote routers connections) which are established.

- **Serial gateway :**

That page displays the current status of the serial gateways :
Type of the gateway(Modbus, RAW, Telnet …),
serial port set-up (data rate etc…),
number of characters received or sent,
Number of TCP frames or UDP datagrams received or sent,
Number of TCP connections enabled.

The View link displays a window which shows the hexadecimal received and transmitted traffic< over each serial COM port.

- **Ping :**

That screen enables to send a ping to an IP address.

- **IO control**

That screen displays the status of the digital input and output and allows to set ON or OFF the alarm digital output.

2 Saving the parameters file

Once a product has been configured, the parameters file can be stored and restored when necessary.

To save the parameters file,

Select the "System" menu and then "Save restore",

Click the "Save" button

Select the location to store the file and give a name to the file.

The file suffix is ".bin".

To restore a parameters file

Select the "System" menu and then "Save restore",

Click the "browse" button and select the parameters file,

Click the "Load" button and confirm to restart the product.

Attention :

A parameters file can only be downloaded to a product having the same firmware version.
It is why, we advise to assign a name to a parameter file including the product name and the software version.
Example :
Name of a parameters file for an IPL-AD2-1220 router with the firmware version V2.41

Example : Myrouterfile_iplad21220_V241.bin

3 Updating the firmware

Step 1 : Before starting, you need,
A PC with a Web browser.

An Ethernet cable or a switch

The FTP server software which can be downloaded from the « firmware page » of the ETIC « download area » web server.

Step 2 : Download the release of the firmware from our download area to your PC

Step 3 : Prepare the PC
Check the Ip address of the PC is compatible with the one of the router.

Connect the router to the PC.

Launch the TFTP server (tftp32.exe) software and select the new release (L026xxx/img) by using the "Browser" button.

Click on "Show dir" to check the files of the directory : rfsmini.tgz, rootfs.bin, u-boot.bin and uImage.

Step 4 : Update the firmware
Launch the web browser

Enter the IP address of the ETIC product ; the home page of the ETIC configuration server is displayed.

Select the "System" menu and then " firmware Update". In the field "IP address of the TFTP server", enter the IP address of your PC.

Note : The IP address of the PC is written in the field "Server Interface" in the TFTP server windows.

Click "Save" and then "Update".

The first file should begin to be downloaded from the PC to the router.

During the operation, the led blinks

When the download is finished, the product automatically reboots.

To be sure the new release has been installed, go to "About" in the administration web page of the IP product.

1/ Setup menu

Remote users
To assign an ID and PWD to each authorized user and set their rights
To set the M2Me service

LAN interface
To enter the IP @ of the router on the LAN interface.
To enter the IP @ assigned to the remote users
To set up the Ethernet interfaces
To set up the DHCP server on the LAN interface

WAN interface
To enter the IP @ of the router over the WAN interface.

Network
To configures the VPNs
To enter static routes and enable the RIP protocol
To set up the VRRP redundancy protocol
To set up port forwarding
To set up advanced Ip addr. translation functions

Security
To set the firewall rules (User filter and main filter)
To add a certificate
To restrict access to the administration server

Alarm
To set up alarm SNMP traps
To set up alarm emails

Serial gateway
To set up the modbus gateway (client / server)
To set up the Unitelway gateway
To set up the RAW TCP / RAW UDP / TELNET gateways

System
To set up SNMP parameters
To enter the devices list
To update the service list
To update time and date

2/ Diagnostic menu

Log	To display the events (VPN connections, user connections..)
Network status	Interfaces status : @ MAC, @IP, ADSL, VPN VPN status Routing tables M2Me_Connect status
Serial gateways	To display the status of each gateway (COM1 and COM2)
Tools	To send Pings from the router
Hardware	To display the input status To control the output To display the DIP switches status
Environment	To display the internal T° and the supply voltage
Advanced	To store the internal report to a disk for diagnostic purposes

3/ Maintenance menu

Firmware update	To update the firmware
Save / restore	To save or restore a configuration file .To restore the factory configuration
Reboot	To restart he router

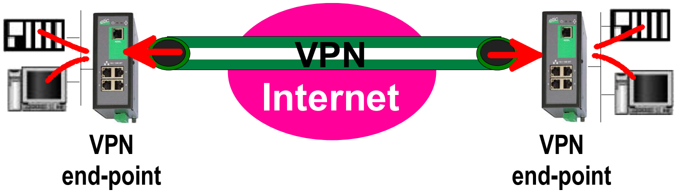
4/ About menu

To display the certificate “product key”
To display the firmware version

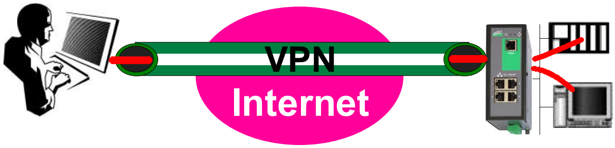
1 Overview

VPN is the acronym for « virtual private network » ; it is a mechanism which allows to connect safely 2 end-points, two routers for instance or one router and one PC, through a network not intrinsically safe.

Once a VPN has been set between two routers , any device of the first network can communicate with any device of the second one as if the two routers were directly connected with an Ethernet cable.



A VPN allows also to connect a remote user to the devices of a network.



2 Functions

A VPN provides the functions described hereafter :

Authentication
The VPN ensures that the party with which the communication is set is actually **the one it claims to be.**

Data integrity
The VPN mechanism ensures that information being transmitted over the public Internet is not altered in any way during transit.

Confidentiality
A VPN protects the privacy of information being exchanged between communicating parties.

3 Operation

Authentication phase

The first operation the end-points carry out is authentication.

2 levels of authentication can be performed using a VPN :

Device level authentication

A code is stored in each end-point (i.e. router or PC); it can be a Key or a certificate delivered by a certification authority.

During the initial phase, the two end-point exchange their codes; each party checks that the other party code is valid.

User level authentication

The IPL-AD2 router holds a user list; once a VPN has been set with the remote user PC, the remote user identification code and password is checked.

Encrypted tunnel transmission phase

Once the end-points have exchanged and checked each other identity code, they set the VPN tunnel.

It is an Ip packets exchange; the source and destination IP addresses are the end-points.

That tunnel encapsulates the encrypted IP data flow transmitted between any of the devices connected to each end-point.

VPN clearing

Periodically, each router (or at least the VPN server router) sends to the other one a control message to check the VPN must remain established.

If no response is received from the other party, the VPN is cleared.

TELECOMMUNICATIONS

13, Chemin du Vieux Chêne

38240 Meylan France

Tel : 33 4 76 04 20 00

Fax : 33 4 76 04 20 01

E-mail : contact@etictelecom.com

Web : www.etictelecom.com